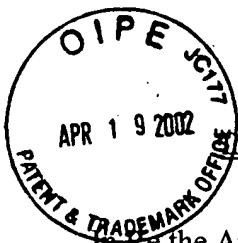


# 4



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re the Application of

: Muneki SHIMADA, et al.

Filed:

: February 20, 2002

For:

: COMPUTER PROGRAM COPY...

Serial No.

: 10/079,935

Assistant Commissioner for Patents  
Washington, D.C. 20231

April 19, 2002

**PRIORITY CLAIM AND**  
**SUBMISSION OF PRIORITY DOCUMENT**

SIR:

Applicant hereby claims priority under 35 USC 119 from JAPANESE patent application no. 2001-044358 filed February 20, 2001 & 2002-041890 filed February 19, 2002, certified copy of which is enclosed.

Any fee, due as a result of this paper may be charged to Deposit Acct. No. 50-1290.

Respectfully submitted,

Thomas J. Bean  
Reg. No. 44,528

KATTEN MUCHIN ZAVIS ROSENMAN  
575 MADISON AVENUE  
IP Department  
NEW YORK, NEW YORK 10022-2584  
DOCKET NO.:100809-00171(SCEY 19.467)  
TELEPHONE: (212) 940-8800



日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office

出願年月日  
Date of Application:

2001年 2月 20日

出願番号  
Application Number:

特願 2001-044358

出願人  
Applicant(s):

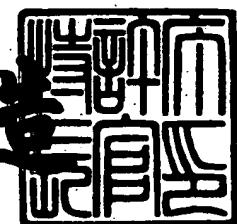
株式会社ソニー・コンピュータエンタテインメント

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2001年12月14日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願  
 【整理番号】 SCEI00263  
 【あて先】 特許庁長官殿  
 【国際特許分類】 G06K 1/00  
 G06N 1/00

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 島田 宗毅

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 岡本 伸一

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 吉森 正治

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 犬井 努

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 島川 恵三

## 【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 岡田 豊史

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 九保 亮

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 中村 光宏

【特許出願人】

【識別番号】 395015319

【氏名又は名称】 株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】 100107238

【弁理士】

【氏名又は名称】 米山 尚志

【手数料の表示】

【予納台帳番号】 111236

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ダウンロード方法及びダウンロードシステム

【特許請求の範囲】

【請求項1】 管理者側において、各記憶媒体に対して固有の識別番号を付すと共に、この記憶媒体に、ダウンロードの対象となるコンテンツを暗号化鍵で暗号化して記憶させ、

ユーザがダウンロードを行う際に使用するダウンロード機器に付された識別番号をユーザ情報として管理者側で登録し、

ユーザがダウンロードを行う際に、上記記憶媒体の識別番号と共に、上記ダウンロード機器の識別番号を管理者側に明示し、

管理者側において、上記ユーザ情報として登録されたダウンロード機器の識別番号と、上記ユーザから明示されたダウンロード機器の識別番号とを照合してユーザを特定し、

管理者側において、上記照合でユーザが特定された際に、その記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵をユーザに配布し

ユーザ側では、管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してダウンロード機器にダウンロードする  
ダウンロード方法。

【請求項2】 管理者側において、上記照合でユーザが特定された際に、この特定されたユーザに対応させて上記記憶媒体の識別番号を登録し、

ユーザがダウンロードを行う際にユーザから明示された上記記憶媒体の識別番号が既に登録済みであるか否かを判別し、

上記記憶媒体の識別番号が未登録であると判別された場合のみ、上記復号化鍵の配布を行うこと

を特徴とする請求項1記載のダウンロード方法。

【請求項3】 管理者側からユーザに対して、上記復号化鍵と共に、上記ユーザ情報として登録されているユーザのダウンロード機器の識別番号を配布し、

ユーザのダウンロード機器は、管理者側から配布された上記ダウンロード機器

の識別番号と、ユーザのダウンロード機器に付されている識別番号とを照合し、両者が一致した場合に、上記復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してダウンロードすること

を特徴とする請求項1又は請求項2記載のダウンロード方法。

【請求項4】 ユーザのダウンロード機器は、その機器に付された識別番号に対応する暗号化用の暗号化鍵を有しており、

管理者側には、上記ユーザのダウンロード機器が有する暗号化用の暗号化鍵と同じ暗号化鍵が、ユーザのダウンロード機器に付された識別番号と共に上記ユーザ情報として登録されており、

明示或いは配布する情報の全部或いは一部を互いに有する上記暗号化用の暗号化鍵に基づいて暗号化して明示或いは配布し、また、暗号化され明示或いは配布された情報を、互いに有する上記暗号化用の暗号化鍵に基づいて復号化して取り込むこと

を特徴とする請求項1から請求項3のうち、いずれか一項記載のダウンロード方法。

【請求項5】 ユーザ側のダウンロード機器において、記憶媒体に記憶されているコンテンツを復号化してダウンロードが終了した後に、このダウンロードするコンテンツを復号化する際に用いた復号化鍵を削除すること

を特徴とする請求項1から請求項4のうち、いずれか一項記載のダウンロード方法。

【請求項6】 管理者側からユーザに対して、上記ダウンロードするコンテンツを再暗号化してダウンロードするための再暗号化鍵を配布し、

ユーザ側では、上記管理者側から配布された再暗号化鍵を用いて、上記記憶媒体の復号化されたコンテンツを再暗号化してダウンロードすると共に、この再暗号化に用いた再暗号化鍵を記憶し、

再生時において、上記再暗号化されダウンロードされたコンテンツを、上記記憶された再暗号化鍵に基づいて復号化して再生すること

を特徴とする請求項1から請求項5のうち、いずれか一項記載のダウンロード方法。

【請求項7】 上記ダウンロード機器が破損し、或いは修理又は交換が必要な場合に、ユーザは、そのダウンロード機器を管理者側に渡し、

管理者側ではユーザから渡されたダウンロード機器に対して修復作業を施し、この修復作業を施したダウンロード機器に新たな識別番号を付すと共に、登録されているユーザ情報の一部或いは全部を、この新たに付した識別番号に応じて書き換えること

を特徴とする請求項1から請求項6のうち、いずれか一項記載のダウンロード方法。

【請求項8】 上記管理者側において、上記記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵をユーザに配布した際に、ユーザに対して課金を行うこと

を特徴とする請求項1から請求項7のうち、いずれか一項記載のダウンロード方法。

【請求項9】 上記管理者側とユーザとの間に介在する中間管理者を設け、この中間管理者を介して管理者側とユーザとの間で情報の受け渡しを行い、

上記中間管理者は、少なくとも上記記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザに対して配布した際に、ユーザに対して課金を行うこと

を特徴とする請求項1から請求項7のうち、いずれか一項記載のダウンロード方法。

【請求項10】 上記記憶媒体は、ユーザに対して無償で配布されることを特徴とする請求項8又は請求項9記載のダウンロード方法。

【請求項11】 管理者側において、各記憶媒体に対してダウンロードの対象となるコンテンツを暗号化鍵で暗号化して記憶させ、

ユーザがダウンロードを行う際に使用するダウンロード機器に付された識別番号をユーザ情報として管理者側で登録し、

ユーザがダウンロードを行う際に、上記ダウンロード機器の識別番号を管理者側に明示し、

管理者側において、上記ユーザ情報として登録されたダウンロード機器の識別

番号と、上記ユーザから明示されたダウンロード機器の識別番号とを照合してユーザを特定し、

管理者側において、上記照合でユーザが特定された際に、その記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵をユーザに配布し

ユーザ側では、管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してダウンロード機器にダウンロードする  
ダウンロード方法。

【請求項12】 上記管理者側において、上記記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵をユーザに配布した際に、ユーザに対して課金を行うこと

を特徴とする請求項11記載のダウンロード方法。

【請求項13】 上記管理者側とユーザとの間に介在する中間管理者を設け、この中間管理者を介して管理者側とユーザとの間で情報の受け渡しを行い、  
上記中間管理者は、少なくとも上記記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザに対して配布した際に、ユーザに対して課金を行うこと

を特徴とする請求項11記載のダウンロード方法。

【請求項14】 上記記憶媒体は、ユーザに対して無償で配布されること  
を特徴とする請求項12又は請求項13記載のダウンロード方法。

【請求項15】 ダウンロードの対象となるコンテンツが暗号化鍵で暗号化されて記憶されると共に、固有の識別番号が付された記憶媒体と、

上記記憶媒体に記憶されたコンテンツのダウンロードを行う際にユーザにより使用され、固有の識別番号が付されたダウンロード機器と、

管理者側に設けられ、ユーザのダウンロード機器に付された識別番号をユーザ情報として記憶するユーザ情報記憶手段と、

管理者側に設けられ、ユーザがダウンロードを行う際に、上記記憶媒体の識別番号と共に、上記ダウンロード機器の識別番号を明示した際に、この明示されたダウンロード機器の識別番号と、上記ユーザ情報記憶手段に記憶されているダウ

ンロード機器の識別番号とを照合してユーザを特定する照合手段と、

管理者側に設けられ、上記照合手段により特定されたユーザに対して、上記記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵を配布する復号化鍵配布手段と、

ユーザのダウンロード機器側に設けられ、上記復号化鍵配布手段により配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してコンテンツのダウンロードを行うダウンロード制御手段と  
を有するダウンロードシステム。

【請求項16】 管理者側に設けられ、上記復号化鍵配布手段により復号化鍵を配布した際に、その復号化鍵を配布した記憶媒体の識別番号を登録し、或いは復号化鍵を配布し記憶媒体の識別番号に復号化鍵が配布されたことを示す情報を付加して登録する配布済み登録手段を有し、

上記復号化鍵配布手段は、上記配布済み登録手段で上記記憶媒体の識別番号が未登録であると判別された場合のみ、上記復号化鍵の配布を行うこと  
を特徴とする請求項15記載のダウンロードシステム。

【請求項17】 上記復号化鍵と共に、上記ユーザ情報として登録されているユーザのダウンロード機器の識別番号を配布する機器番号配布手段を有し、

上記ダウンロード制御手段は、上記機器番号配布手段から配布された上記ダウンロード機器の識別番号と、ユーザのダウンロード機器に付されている識別番号とを照合し、両者が一致した場合に、上記復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してダウンロードすること  
を特徴とする請求項16又は請求項17記載のダウンロードシステム。

【請求項18】 ユーザのダウンロード機器は、その機器に付された識別番号に対応する暗号化用の暗号化鍵を有しており、

管理者側には、上記ユーザのダウンロード機器が有する暗号化用の暗号化鍵と同じ暗号化鍵が、ユーザのダウンロード機器に付された識別番号と共に上記ユーザ情報記憶手段に記憶されており、

明示或いは配布する情報の全部或いは一部を互いに有する上記暗号化用の暗号化鍵に基づいて暗号化して明示或いは配布し、また、暗号化され明示或いは配布

された情報を、互いに有する上記暗号化用の暗号化鍵に基づいて復号化して取り込むこと

を特徴とする請求項15から請求項17のうち、いずれか一項記載のダウンロードシステム。

【請求項19】 上記ダウンロード制御手段は、記憶媒体からのダウンロードが終了した後に、このダウンロードしたコンテンツを復号化する際に用いた復号化鍵を削除すること

を特徴とする請求項15から請求項18のうち、いずれか一項記載のダウンロードシステム。

【請求項20】 管理者側に設けられ、上記ダウンロードするコンテンツを再暗号化してダウンロードするための再暗号化鍵を配布する再暗号化鍵配布手段と、

ユーザのダウンロード機器側に設けられ、上記再暗号化鍵配布手段により配布された再暗号化鍵を記憶する再暗号化鍵記憶手段と、

ユーザのダウンロード機器側に設けられ、上記再暗号化鍵記憶手段に記憶された再暗号化鍵を用いて、上記ダウンロードされるコンテンツを再暗号化する再暗号化手段と、

ユーザのダウンロード機器側に設けられ、上記再暗号化手段により再暗号化されダウンロードされたコンテンツを、上記記憶された再暗号化鍵に基づいて復号化して再生する再生手段と

を有することを特徴とする請求項15から請求項19のうち、いずれか一項記載のダウンロードシステム。

【請求項21】 上記ダウンロード機器が破損し、或いは修理又は交換が必要な場合に、ユーザは、そのダウンロード機器を管理者側に渡し、

管理者側ではユーザから渡されたダウンロード機器に対して修復作業を施し、この修復作業を施したダウンロード機器に新たな識別番号を付すと共に、登録されているユーザ情報の一部或いは全部を、この新たに付した識別番号に応じて書き換えること

を特徴とする請求項15から請求項20のうち、いずれか一項記載のダウンロ

ードシステム。

【請求項22】 上記管理者側に設けられ、上記復号化鍵配布手段によりユーザに対して復号化鍵が配布された際に、ユーザに対して課金を行う課金手段を有すること

を特徴とする請求項15から請求項21のうち、いずれか一項記載のダウンロードシステム。

【請求項23】 上記管理者側とユーザとの間の情報の受け渡しを仲介し、少なくとも上記記憶媒体に記憶されているコンテンツを復号化するための復号化鍵をユーザに対して配布した際に、ユーザに対して課金を行う仲介手段を有すること

を特徴とする請求項15から請求項21のうち、いずれか一項記載のダウンロードシステム。

【請求項24】 上記記憶媒体は、ユーザに対して無償で配布されることを特徴とする請求項22又は請求項23記載のダウンロードシステム。

【請求項25】 ダウンロードの対象となるコンテンツが暗号化鍵で暗号化されて記憶された記憶媒体と、

上記記憶媒体に記憶されたコンテンツのダウンロードを行う際にユーザにより使用され、固有の識別番号が付されたダウンロード機器と、

管理者側に設けられ、ユーザのダウンロード機器に付された識別番号をユーザ情報として記憶するユーザ情報記憶手段と、

管理者側に設けられ、ユーザがダウンロードを行う際に、上記ダウンロード機器の識別番号を明示した際に、この明示されたダウンロード機器の識別番号と、上記ユーザ情報記憶手段に記憶されているダウンロード機器の識別番号とを照合してユーザを特定する照合手段と、

管理者側に設けられ、上記照合手段により特定されたユーザに対して、上記記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵を配布する復号化鍵配布手段と、

ユーザのダウンロード機器側に設けられ、上記復号化鍵配布手段により配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化して

コンテンツのダウンロードを行うダウンロード制御手段と  
を有するダウンロードシステム。

【請求項26】 上記管理者側に設けられ、上記記憶媒体に暗号化され記憶  
されているコンテンツを復号化するための復号化鍵をユーザに配布した際に、ユ  
ーザに対して課金を行う課金手段を有すること  
を特徴とする請求項25記載のダウンロードシステム。

【請求項27】 上記管理者側とユーザとの間に介在して管理者側とユーザ  
との間で情報の受け渡しを行うと共に、少なくとも上記記憶媒体に記憶されてい  
るコンテンツを復号化するための復号化鍵をユーザに対して配布した際に、ユー  
ザに対して課金を行う仲介手段を有すること  
を特徴とする請求項25記載のダウンロードシステム。

【請求項28】 上記記憶媒体は、ユーザに対して無償で配布されること  
を特徴とする請求項26又は請求項27記載のダウンロードシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えばCD-ROM, CD-R, CD-RW, DVD-ROM, D  
VD-RAM等の第1の記憶媒体から、ハードディスク(HD), 光磁気ディス  
ク(MO), DVD-ROM等の第2の記憶媒体にインストールされたゲームコ  
ンテンツ、音楽コンテンツ、映画コンテンツ等のデジタルコンテンツの不正使用  
の防止等を図ったダウンロード方法及びダウンロードシステムに関する。

【0002】

【従来の技術】

今日において、例えばCD-ROM, DVD-ROM或いは半導体メモリ等の  
記憶媒体に記憶されているゲームプログラムに基づいてビデオゲームを実行する  
ビデオゲーム機が広く普及している。

【0003】

ユーザは、所望のゲームプログラムが記憶された記憶媒体を購入し、この記憶  
媒体をビデオゲーム機で再生してビデオゲームを行うのであるが、大抵の場合、

徐々に新しいビデオゲームを買い揃えていくため、月日と共にユーザの手元には各ゲームプログラムが記憶された記憶媒体が蓄積されていくこととなる。

#### 【0004】

ビデオゲーム機には、記憶媒体の再生機構が1基のみ設けられている場合が多い。このため、異なるビデオゲームを行う場合には、ビデオゲーム機に現在装着されている記憶媒体を取り出し、これから行おうとするゲームプログラムが記憶された記憶媒体を新たに装着し直すという、大変面倒な作業を必要としていた。

#### 【0005】

##### 【発明が解決しようとする課題】

このため、本件出願人は、例えば数十G（ギガ）オーダーの大容量のハードディスクドライブ（HDD）をビデオゲーム機に内蔵或いは外付けし、このHDDに各記憶媒体に記憶されているゲームプログラムをダウンロードして再生可能としたビデオゲーム機を開示している。

#### 【0006】

これにより、各記憶媒体に記憶されているゲームプログラムを一括してHDDに記憶させ、このHDDから所望のゲームプログラムを再生して利用することができるため、異なるビデオゲームを行おうとする毎にそのゲームプログラムが記憶された記憶媒体を再生機構から着脱する手間を省略することができる。

#### 【0007】

ここで、ビデオゲーム等のデジタルコンテンツの利用は、そのデジタルコンテンツを購入する等して正当に入手したユーザのみが利用可能のはずである。しかし、このようにCD-ROMやDVD-ROM等の記憶媒体に記憶されたデジタルコンテンツを、ハードディスクや光磁気ディスク等の記憶媒体にインストールして再生可能とした場合、このデジタルコンテンツが記憶されたCD-ROMやDVD-ROM等を他のユーザに貸与することで、他のユーザも自分のハードディスクドライブにこのデジタルコンテンツをインストールして不正に利用可能となり好ましいことではない。

#### 【0008】

すなわち、1つの記憶媒体があれば、この記憶媒体に記憶されているデジタル

コンテンツを他のユーザが自分のハードディスク等の記憶媒体にインストールすることで、次々と連鎖的な不正使用が可能となり、好ましいことではない。

【0009】

本発明は上述の課題に鑑みてなされたものであり、光ディスク等の第1の記憶媒体からハードディスク等の第2の記憶媒体へのデジタルコンテンツのダウンロードを正当なユーザに対してのみ可能とすることで、第1の記憶媒体に記憶されたデジタルコンテンツの不正使用を防止することができるようなダウンロード方法及びダウンロードシステムの提供を目的とする。

【0010】

【課題を解決するための手段】

本発明は、各記憶媒体に対してそれぞれ固有の識別番号を付すと共に、この記憶媒体に、ダウンロードの対象となるコンテンツを暗号化鍵で暗号化して記憶させてユーザに配布する。ユーザがダウンロードを行う際に使用するダウンロード機器にも識別番号が付されており、管理者側では、このダウンロード機器の識別をユーザ情報として登録して管理する。

【0011】

ユーザがダウンロードを行う際に、上記記憶媒体の識別番号と共に、上記ダウンロード機器の識別番号を管理者側に明示すると、管理者側では、予めユーザ情報として登録されているダウンロード機器の識別番号と、ユーザから明示されたダウンロード機器の識別番号とを照合してユーザを特定する。そして、この照合によりユーザが特定された際に、記憶媒体に暗号化され記憶されているコンテンツを復号化するための復号化鍵をユーザに配布する。

【0012】

ユーザは、この管理者側から配布された復号化鍵に基づいて上記記憶媒体に記憶されているコンテンツを復号化してダウンロード機器にダウンロードする。

【0013】

これにより、ユーザが使用しているダウンロード機器と、ダウンロードを行うコンテンツが記録された記録媒体を特定したうえで、記憶媒体からのダウンロードを許可することができる。

【0014】

すなわち、記憶媒体の持ち主である正規のユーザにのみ、このダウンロードを許可することで、記憶媒体に記憶されたコンテンツの不正使用を防止している。

【0015】

【発明の実施の形態】

本発明は、DVD-ROM, CD-ROM, 半導体メモリ等の第1の記憶媒体に記録されているゲームプログラム、映画コンテンツ、音楽コンテンツ等のデジタルコンテンツを、ハードディスク(HD)や光磁気ディスク(MO)等の第2の記憶媒体にダウンロードする際に、システムサーバ装置側から提供された暗号化鍵(暗号キー)を用いてダウンロードを行うダウンロードシステムに適用することができる。

【0016】

なお、デジタルコンテンツが記憶されている第1の記憶媒体としては、DVD-ROM, CD-ROM, 半導体メモリ等、何でもよいのであるが、この例においては、一例としてDVD-ROMやCD-ROM等の光ディスクにデジタルコンテンツが記憶されているものとして説明を行うこととする。

【0017】

同様に、デジタルコンテンツをダウンロードする第2の記憶媒体としても、ハードディスク(HD)や光磁気ディスク(MO)等、何でもよいのであるが、この例においては、一例として上記光ディスクからのデジタルコンテンツをハードディスク(HD)にダウンロードするものとして説明を行うこととする。

【0018】

【ダウンロードシステムの全体構成】

まず、図1に本発明の第1の実施の形態となるダウンロードシステムの全体構成を示す。この図1からわかるように、この第1の実施の形態のダウンロードシステムは、少なくともビデオゲームの実行機能及びネットワークを介した通信機能を備えたクライアント端末装置1を有している。このクライアント端末装置1には、このクライアント端末装置1に装着された光ディスクに記憶されているゲームプログラムをダウンロードするためのハードディスクドライブ2(HDD)

と、クライアント端末装置1と上記ネットワークとの接続を図る通信モデム6とが接続されている。

#### 【0019】

なお、通信モデム6は、この図1に示すようにクライアント端末装置1に対して外付けのかたちで設けても、クライアント端末装置1に内蔵のかたちで設けてもよい。

#### 【0020】

また、ダウンロードシステムは、後に説明するユーザエントリ情報が記憶されたデータベース3を備えたシステムサーバ装置4を有しており、このシステムサーバ装置4と上記クライアント端末装置1とが、例えばインターネット5等のネットワークを介して相互に接続されることでこの第1の実施の形態のダウンロードシステムが構成されている。

#### 【0021】

##### 【クライアント端末装置の構成】

図2に、クライアント端末装置1の外観の斜視図を示す。この図2からわかるように、クライアント端末装置1の前面側には、コントローラ接続部7A、7Bと、メモリカード装着部8A、8Bと、USB対応機器（USB：Universal Serial Bus）が接続される2つのUSB接続端子9と、例えば最大400Mbpsのデータ転送速度に対応可能なIEEE1394接続端子10とが設けられている。

#### 【0022】

また、このクライアント端末装置1の前面側には、ビデオゲームのゲームプログラムや映画コンテンツ等のデジタルコンテンツが記憶されたCD-ROMやDVD-ROM等の光ディスクが装着されるトレイ型のディスク装着部11と、ゲームをリセットするためのリセットボタン12と、光ディスク装着部11のトレイの出し入れを操作するためのトレイ操作ボタン13とが設けられている。

#### 【0023】

これに対して、このクライアント端末装置1の背面側には、電源スイッチ、音声映像出力端子（AVマルチ出力端子）、PCカードスロット、光デジタル出力

端子、AC電源入力端子等が設けられている。

#### 【0024】

AVマルチ出力端子は、AVケーブル17を介してモニタ用のテレビジョン受像機18に接続されるようになっており、ビデオゲームの映像信号や音声信号を、このAVマルチ出力端子及びAVケーブル17を介してモニタ用のテレビジョン受像機18に供給することで、ビデオゲームの映像をテレビジョン受像機18に表示し、ビデオゲームの音声をテレビジョン受像機のスピーカ装置を通して発音するようになっている。

#### 【0025】

コントローラ接続部7A、7Bには、コントローラケーブル15を介してそれぞれコントローラ14を接続することができるようになっており、2人のプレイヤーが同時に、或いは一人ずつ交代でビデオゲームを行うことができるようになっている。

#### 【0026】

また、メモリカード装着部8A、8Bには、ゲームデータのセーブ（記憶）及び読み出しを行うセーブ用のメモリカード等を装着するようになっている。

#### 【0027】

##### 〔ハードディスクドライブの構成〕

次に、図2において、クライアント端末装置1の上面部に載置されている筐体がハードディスクドライブ2（HDD）である。このHDD2は、内部に例えば40GB等の大容量のハードディスクが設けられており、後に説明するようにDVD-ROMに記憶されているゲームプログラムをインストールした場合、十数枚分のDVD-ROMのゲームプログラムを記憶可能となっている。

#### 【0028】

また、このHDD2の前面側には、電源投入時に点灯駆動される電源ランプ20と、ハードディスクへの書き込みに連動して点灯駆動される書き込み表示ランプ21とが設けられている。これに対して、このHDD2の背面側には、少なくとも電源スイッチ及びデータ入出力端子が設けられている。

#### 【0029】

このHDD2をクライアント端末装置1に接続する場合、クライアント端末装置1の背面側に設けられた上記PCカードスロットにPCカードを挿入し、このPCカードに接続ケーブルの一端を接続する。そして、この接続ケーブルの他端をHDD2のデータ入出力端子に接続する。これにより、クライアント端末装置1とHDD2とが、電気的に相互に接続されるようになっている。

#### 【0030】

なお、この例においては、HDD2はクライアント端末装置1とは別体で、クライアント端末装置1に対して外付けのかたちで接続されることとして説明を進めているが、このHDD2は、クライアント端末装置1に内蔵されるかたちで設けるようにしてもよい。

#### 【0031】

また、クライアント端末装置1とHDD2とをPCカードと接続ケーブルを介して接続することとして説明を進めているが、HDD2の背面側（或いは前面側でもよい。）にUSB接続端子やIEEE1394接続端子等の接続端子を設け、この接続端子を介してHDD2をクライアント端末装置1に接続するようにしてもよい。

#### 【0032】

##### 〔クライアント端末装置の電気的構成〕

次に、図3はクライアント端末装置1のブロック図である。この図3からわかるようにクライアント端末装置1は、CPU30と、グラフィックプロセッサ31（GPU）と、I/Oプロセッサ32（IOP）と、CD-ROMやDVD-R OM等の光ディスクの再生制御を行う光ディスク制御部33と、サウンドプロセッサユニット34（SPU）と、CPU30やIOP32が実行するオペレーティングシステムプログラムが格納されたMASK-ROM35と、CPU30のワークエリアや光ディスクから読み出されたデータを一時的に格納するバッファとして機能するRAM36とを有している。

#### 【0033】

また、このクライアント端末装置1は、光ディスク制御部33のRFアンプ37を介して供給される光ディスクからの再生出力に対して、例えば誤り訂正処理

(C I R C処理) 等を施して出力するCD/DV D D S P 3 8と、光ディスク制御部3 3のスピンドルモータの回転制御、光ピックアップのフォーカス/トラッキング制御、ディスクトレーのローディング制御等を行うドライバ3 9及びメカコントローラ4 0と、上記H D D 2を当該クライアント端末装置1に接続するためのP Cカードが接続されるカード型コネクタ4 1とを有している。これらの各部は、主にバスライン4 2、4 3等を介してそれぞれ相互に接続されている。

#### 【0034】

なお、D V D - R O Mに記憶された映画コンテンツの再生は、メモリカードに記憶されたD V D ドライバ、或いはクライアント端末装置1内に内蔵された半導体メモリ4 4 (DVD Player ROM) に焼き付けられD V D ドライバに基づいて行われるようになっている。

#### 【0035】

このようなクライアント端末装置1において、C P U 3 0は、M A S K - R O M3 5に記録されているオペレーティングシステムプログラムを実行することにより、このクライアント端末装置1全体を制御するようになっている。

#### 【0036】

M A S K - R O M3 5には、コントローラ接続部7 A、7 Bと、メモリカード装着部8 A、8 B、及びカード型コネクタ4 1に接続されるコントローラ1 4、メモリカード1 6及びH D D 2等のデバイス識別番号(デバイスI D)も記憶されている。I O P 3 2は、このM A S K - R O M3 5に記憶されているデバイスI Dに基づいて、コントローラ1 4、メモリカード1 6及びH D D 2等のデバイスと通信を行い、各接続端子7 A、7 B、8 A、8 B及びカード型コネクタ4 1等に接続されたデバイスを認識するようになっている。

#### 【0037】

なお、ここでいうデバイスI Dは、各クライアント端末装置1毎、各メモリカード1 6毎、或いは各H D D 2毎に異なるように付された各デバイス固有のI D(後にクライアントI D、MC-I D及びH D D - I Dとして説明する。)とは異なり、全てのクライアント端末装置1、全てのメモリカード1 6、全てのH D D 2がそれぞれ同一となるように付されたI Dである。

## 【0038】

すなわち、デバイスIDは、クライアント端末装置1全体で一つのID、メモリカード16全体で一つのID、及びHDD2全体で一つのID等のように、いわば各デバイスの総称のようなかたちで付されたIDを意味しており、これに対して、クライアントID、MC-ID及びHDD-IDは、各クライアント端末装置1毎、各メモリカード16毎、及び各HDD2毎にそれぞれ付された各デバイス固有のIDとなっている。

## 【0039】

IOP32は、まず、MASK-ROM35から各デバイスIDを読み出して、このデバイスIDに基づいて各接続端子7A、7B、8A、8B及びカード型コネクタ41等に接続されたデバイスを認識し、このデバイスの認識をしたうえで新たに各デバイスと通信を行い、各デバイス固有のIDを取り込んで、各メモリカード16毎、各HDD2毎等の識別を行うようになっている。

## 【0040】

次に、GPU31は、CPU30からの描画指示に従って描画を行い、描画された画像を図示しないフレームバッファに格納する。また、GPU31は、座標変換等の処理を行なうジオメトリransferエンジンとしての機能を有している。

## 【0041】

具体的には、このジオメトリransferエンジンとして機能するGPU31は、例えば光ディスクに記録されているゲームプログラムがいわゆる3Dグラフィックを利用する場合に、三角形状のポリゴンの集合で仮想的な3次元オブジェクトを構成する。そして、この3次元オブジェクトを仮想的なカメラ装置で撮影することで得られる画像を生成するための諸計算、すなわち、レンダリングを行う場合における透視変換処理（3次元オブジェクトを構成する各ポリゴンの頂点を仮想的なカメラスクリーン上に投影した場合における座標値の計算）等を行う。

## 【0042】

また、GPU31は、CPU30からの描画指示に従って、必要に応じてジオ

メトリトランスファエンジンを利用しながら、フレームバッファに対して3次元オブジェクトのレンダリングを行い画像を形成する。そして、この形成した画像に対応するビデオ信号（visual out）を出力するようになっている。

#### 【0043】

一方、SPU34は、適応予測符号化された音声データを再生するADPCM復号機能と、サウンドバッファに記憶されている波形データを再生することで、効果音等の音声信号を再生して出力（audio out）する再生機能と、サウンドバッファに記憶されている波形データを変調させて再生する変調機能等を備えており、CPU30からの指示によりサウンドバッファに記憶されている波形データに基づき楽音、効果音等の音声信号を発生する、いわゆるサンプリング音源として使用することができるようになっている。

#### 【0044】

このようなクライアント端末装置1は、電源が投入されると、CPU30及びIOP32が、MASK-ROM35からCPU30用のオペレーティングシステムプログラム及びIOP32用のオペレーティングシステムプログラムをそれぞれ読み出し、このオペレーティングシステムプログラムに基づいてCPU30及びIOP32が動作するようになっている。そして、CPU30によりクライアント端末装置1の各部が統括的に制御され、また、IOP32によりコントローラ14、メモリカード16、及びHDD2等との間のデータの入出力が制御されるようになっている。

#### 【0045】

また、CPU30は、オペレーティングシステムプログラムに基づいて、動作確認等の初期化処理を行った後、光ディスク制御部33を制御し、光ディスクに記録されているビデオゲーム等のゲームプログラムを実行し、或いは光ディスクに記録されている映画等の再生し、さらには、光ディスクから再生されたゲームコンテンツや映画コンテンツ等のデジタルコンテンツをHDD2にインストール制御するようになっている。

#### 【0046】

このビデオゲームのゲームプログラムを実行する場合、CPU30は、IOP

32を介してコントローラ14から受け付けたプレーヤからの指示（コマンド）に従ってGPU31やSPU34を制御し、ゲーム画像の表示や効果音、楽音の発生を制御する。

## 【0047】

また、映画の再生を行う場合も同様であり、CPU30は、IOP32を介してコントローラ14受け付けたプレーヤからの指示に従ってGPU31やSPU34を制御し、光ディスクから再生された映画の映像の表示や音声の発生等を制御するようになっている。

## 【0048】

## 【光ディスクからHDDへのインストール制御】

次に、このようなダウンロードシステムは、光ディスクに記憶されているゲームプログラムや映画コンテンツ等のデジタルコンテンツをHDD2にインストール可能とすることで懸念されるデジタルコンテンツの不正使用を以下のように防止している。

## 【0049】

## (インストーラのインストール)

まず、このダウンロードシステムにおいて、クライアント端末装置1からHDD2へのデジタルコンテンツのダウンロードを可能とするためには、クライアント端末装置1にダウンロード用のアプリケーションプログラム（インストーラ）をインストールする必要がある。

## 【0050】

この例の場合、インストーラは各デジタルコンテンツと共に光ディスクに記憶、或いはシステム業者側から配布される光ディスクに記憶されている。このインストーラのインストールを行う場合、ユーザは、インストーラが記憶されている光ディスクをクライアント端末装置1に装着する。クライアント端末装置1は、この光ディスクが装着されると自動的に（オートラン）、或いはユーザのコントローラ14の操作に従って光ディスクに記憶されているインストーラを読み出し、これをメモリカード16或いはRAM36に記憶制御する。

## 【0051】

このメモリカード16或いはRAM36に記憶されたインストーラは、光ディスクに記憶されているデジタルコンテンツをHDD2にダウンロードする際に読み出され、このインストーラに基づいてCPU30がダウンロード制御を行う。

## 【0052】

なお、インストーラは、一例として各デジタルコンテンツと共に光ディスクに記憶されており、或いはシステム業者側から配布される光ディスクに記憶されていることとしたが、予めインストーラが記憶されたメモリカード16を配布し、或いはインストーラが記憶されたROMをクライアント端末装置1内に設けてもよい。これにより、ユーザによるインストーラのインストール作業を省略可能とすることができる。

## 【0053】

## (デジタルコンテンツの暗号化記録)

次に、このダウンロードシステムにおいては、図4に示すようにゲームプログラムや映画コンテンツ等のデジタルコンテンツが、各デジタルコンテンツ毎に異なる対称鍵（コンテンツキー：Content-Key）により暗号化され光ディスクに記憶されている。また、この光ディスクには、このように暗号化されたデジタルコンテンツの他、各光ディスク毎に異なるように付された各光ディスク固有のIDである「Media unique ID（メディアユニークID：MID）」が記録されている。

## 【0054】

## (ユーザ登録)

このような光ディスクからデジタルコンテンツをHDD2にダウンロードする場合、この第1の実施の形態のダウンロードシステムにおいては、各メモリカード16に個別に付されている識別番号である「メモリカードID（MC-ID）」を用いてシステムサーバ装置4にユーザ登録を行わなければHDD2に対してデジタルコンテンツをダウンロードできないようになっている。

## 【0055】

図5は、ユーザがシステムサーバ装置4に対してユーザ登録を行うまでの流れを示すフローチャート、図6は、このユーザ登録によりクライアント端末装置1

とシステムサーバ装置4との間で送受信される情報を示す当該ダウンロードシステムの模式図である。

#### 【0056】

この図5及び図6を用いてユーザ登録動作を説明すると、まず、図5のフローチャートは、ユーザがクライアント端末装置1のメイン電源を投入することでスタートとなり、このユーザ登録の行程がステップS1に進む。

#### 【0057】

ステップS1では、ユーザがインターネット5を介して自分のクライアント端末装置1をシステムサーバ装置4に接続する。

#### 【0058】

具体的には、このクライアント端末装置1には、図1に示したようにインターネット接続用の通信モデム6が接続（或いは内蔵）されており、ユーザによりインターネット接続が指定されると、図3に示すCPU30が所定のWWWブラウザに基づいて動作し、通信モデム6を介して当該クライアント端末装置1とシステムサーバ装置4との間の通信回線の確立を図る。これにより、このユーザ登録の行程がステップS2に進む。

#### 【0059】

ステップS2では、ユーザが、クライアント端末装置1に装着されたメモリカードの識別番号(MC-ID)、クライアント端末装置1毎に付された固有の識別番号(クライアントID)及びHDD2毎に付された固有の識別番号(HDD-ID)をシステムサーバ装置4側に送信する。

#### 【0060】

具体的には、CPU30はシステムサーバ装置4とクライアント端末装置1との通信回線が確立されると、クライアント端末装置1、HDD2及びメモリカード16とそれぞれ通信を行い、各デバイスからクライアント端末装置1毎に付された固有の識別番号(クライアントID)、HDD2毎に付された固有の識別番号(HDD-ID)、及びクライアント端末装置1に装着されたメモリカード16固有の識別番号(MC-ID)をそれぞれ自動的に取得し、これらを図6に示すようにシステムサーバ装置4側に送信する。これにより、このユーザ登録の行

程がステップS3に進む。

#### 【0061】

なお、クライアント端末装置1、HDD2及びメモリカード16には、クライアントID、HDD-ID及びMC-IDがそれぞれ各筐体にユーザが黙視可能なかたちで張り付けられている。このため、この例においては、クライアントID、HDD-ID及びMC-IDは、CPU30が各デバイスと通信を行い自動的に取得してシステムサーバ装置4側に送信することとしたが、これは、システムサーバ装置4とクライアント端末装置1との通信回線が確立された際に、図1に示すテレビジョン受像機18の表示画面に、例えば「ユーザ登録をして下さい」等のユーザ登録を促すメッセージを表示制御し、ユーザがコントローラ14を操作してクライアントID、HDD-ID及びMC-IDの入力を行い、CPU30が、この入力されたクライアントID、HDD-ID及びMC-IDをシステムサーバ装置4側に送信するようにしてもよい。

#### 【0062】

また、クライアント端末装置1とシステムサーバ装置4との間においては、例えばSSL(Secure Sockets Layer)等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

#### 【0063】

ステップS3では、システムサーバ装置4が、このユーザ側から送信されたメモリカードの識別番号(MC-ID)が有効なIDであるか否かを判別し、有効なIDである場合は、このユーザ登録の行程がステップS4に進み、無効なIDである場合は、このユーザ登録の行程がステップS7に進む。

#### 【0064】

具体的には、このダウンロードシステムの一部を構成するクライアント端末装置1、HDD2及びメモリカード16は、それぞれ前述のように固有のIDが付されているのであるが、システムサーバ装置4側のデータベース3には、各クライアント端末装置1、各HDD2及び各メモリカード16にそれぞれ付されている固有のIDが全て記憶されている。

#### 【0065】

このため、システムサーバ装置4は、ユーザ側からクライアント端末装置1、HDD2及びメモリカード16の各固有のIDが送信されると、まず、ユーザ側から送信されたメモリカード16の固有のIDであるMC-IDと、データベース3に登録されている各MC-IDとを照合し、ユーザ側から送信されたメモリカード16のMC-IDと同じMC-IDがデータベース3に登録されているか否か、すなわち、ユーザ側から送信されたメモリカード16のMC-IDは、データベース3に正規に登録されているMC-IDと同じであるか否かを判別する。

#### 【0066】

そして、ユーザ側から送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれのMC-IDとも一致しなかった場合には、システムサーバ装置4は、このユーザ登録のアクセスを不正なユーザ登録のアクセスと見なし、ステップS7において、例えば「このメモリカードではユーザ登録を行うことはできません。」等のユーザ登録を拒否するメッセージをクライアント端末装置1側に返信する（無効通知）。これにより、ユーザ登録が中断されたかたちで、このユーザ登録行程が終了することとなる。

#### 【0067】

一方、ユーザ側から送信されたメモリカード16のMC-IDが、データベース3に正規に登録されているいずれかのMC-IDと一致した場合には、ステップS4において、システムサーバ装置4が、現在、システムサーバ装置4にアクセスしているユーザの固有のIDであるユーザID（User ID）を、例えば乱数等を用いて形成する。

#### 【0068】

そして、図6に示すようにそのユーザのクライアントID、HDD-ID及びMC-IDと共に、上記ユーザの固有のIDであるユーザID（User ID）、及び後に説明するMC-Keyを一総めにし、これを「ユーザエントリ情報」としてシステムサーバ装置4のデータベース3に登録する。

#### 【0069】

これにより、各ユーザが所有するクライアント端末装置1、HDD2及びメモ

リカード16の3つのIDの組み合わせで各ユーザを特定してデータベース3に登録することができる。

## 【0070】

すなわち、クライアント端末装置1、HDD2及びメモリカード16の3つのIDが、異なるユーザ間で全て一致するということは有り得ないため、この3つのIDに基づいてユーザ登録を行うことにより、確実にユーザを特定してユーザ登録を行うことができる。これにより、後述する光ディスクに記録されたコンテンツの不正なダウンロードを、より強力に防止することができる。

## 【0071】

なお、ユーザ登録の際に、「MC-IDのみ」、「クライアントIDのみ」、「HDD-IDのみ」、「MC-IDとクライアントID」、「MC-IDとHDD-ID」、或いは「クライアントIDとHDD-ID」をシステムサーバ装置4側に送信してユーザ登録を行うようにしてもよい。これらの場合でも、各IDはそれぞれ固有のIDであるため、異なるユーザ間で重複することではなく、略々確実にユーザを特定してユーザ登録を行うことができる。

## 【0072】

次に、ユーザ登録の行程がステップS5に進むと、システムサーバ装置4が、ユーザ登録が正規に完了した証として、上記ステップS4で形成したユーザエントリ情報のうち、ユーザID(User ID)をMC-Keyで暗号化し、これをクライアント端末装置1側に返信する。

## 【0073】

(MC-Key)

ここで、上記「MC-Key」なのであるが、これは、クライアント端末装置1とシステムサーバ装置4との間で送受信する情報を暗号化するための鍵情報であり、MC-IDと共にメモリカード16内に予め記憶されている。

## 【0074】

MC-IDは、ユーザが黙視可能なようにメモリカード16の筐体に張り付けられているのに対して、このMC-Keyはユーザが黙視できないようにメモリカード16内に記憶されている。また、このMC-Keyは、ユーザがメモリカ

ード16内に記憶されている情報を再生した場合でも表示や出力が行われることのない秘密性のある鍵情報となっており、ユーザが認識することはできないようになっている。

#### 【0075】

また、このダウンロードシステムの場合、MC-IDは前述のようにユーザ登録の際にクライアントID及びHDD-IDと共にシステムサーバ装置4側に送信されるのに対して、このMC-Key自体は、クライアント端末装置1とシステムサーバ装置4との間で送受信されることはないようになっている。

#### 【0076】

すなわち、このダウンロードシステムの場合、MC-Keyは、MC-IDと共にメモリカード16内に予め記憶されているのであるが、システムサーバ装置4のデータベース3にも、各メモリカード16のMC-ID及びMC-Keyがそれぞれ記憶されている。言い換えれば、クライアント端末装置1及びシステムサーバ装置4は、各メモリカード16に対応するMC-ID及びMC-Keyをそれぞれ有している。

#### 【0077】

このため、クライアント端末装置1からシステムサーバ装置4にMC-Keyを送信する必要はなく、システムサーバ装置4は、予めデータベース3に記憶されているMC-Keyの中から、現在アクセスされているユーザのメモリカード16に対応するMC-Keyを選択し、このMC-Keyを用いてユーザID(User ID)を暗号化してクライアント端末装置1側に返信する。

#### 【0078】

このMC-Keyは、上記ユーザID(User ID)や、後に説明する光ディスク固有のIDであるメディアユニークID(media unique ID(MID))、光ディスクにデジタルコンテンツを暗号化して記録する際に用いられたコンテンツキー(Content-Key)、及びHDD2にデジタルコンテンツをダウンロードする際に、このデジタルコンテンツを再暗号化するために用いられる「Content-Gen-Key」をそれぞれ復号化する際に用いられるようになっている。

## 【0079】

このため、このようにクライアント端末装置1とシステムサーバ装置4との間におけるMC-Keyの送受信を不要とすることで、MC-Keyが第三者に不正に略取される不都合を防止することができ、このダウンロードシステムにおけるデジタルコンテンツのHDD2への不正なダウンロードを強力に防止することができる。

## 【0080】

次に、ユーザ登録行程がステップS6に進むと、クライアント端末装置1が、システムサーバ装置4側から返信されたユーザID(User ID)をメモリカード16に記憶制御する。これにより、この図5のフローチャートに示すユーザ登録の全行程が終了する。そして、この時点において、メモリカード16には、図6に示すように予め記憶されているMC-ID及びMC-Keyと共に、MC-Keyで暗号化されたユーザID(User ID)が記憶されることとなる。

## 【0081】

(メディアユニークIDの登録とコンテンツキーの取得)

次に、光ディスクに記録されているデジタルコンテンツを何ら制限無く何回でもHDD2にダウンロード可能とすると、MC-ID, MC-Key及びユーザID(User ID)が記録されたメモリカード16を他のユーザに貸与するだけで、この他のユーザも光ディスクに記録されているデジタルコンテンツをこの他のユーザのHDDに不正にダウンロード可能となり好ましいことではない。

## 【0082】

このため、このダウンロードシステムでは、各光ディスク毎に付されている固有のIDであるメディアユニークID(media unique ID(MI-D))をシステムサーバ装置4に登録させ、同じメディアユニークIDを有する光ディスクからは一度しかデジタルコンテンツのダウンロードを許可しないようにして、光ディスクからHDD2へのデジタルコンテンツのダウンロードを一回に制限するようになっている。

## 【0083】

また、光ディスクに記録されているデジタルコンテンツは、前述のようにコンテンツキー（Content Key）により暗号化されているため、この暗号化されているデジタルコンテンツを復号化するためには、システムサーバ装置4側から復号化のためのコンテンツキーを取得する必要がある。

#### 【0084】

このため、このダウンロードシステムでは、正規のユーザからデジタルコンテンツのダウンロード要求があった場合には、コンテンツキー（Content Key）をそのユーザに対して提供するようになっている。

#### 【0085】

図7は、メディアユニークID（MID）の登録とユーザがコンテンツキーを取得するまでの流れを示すフローチャート、図8は、このメディアユニークIDの登録とコンテンツキーの取得の際にクライアント端末装置1とシステムサーバ装置4との間で送受信される情報を示す当該ダウンロードシステムの模式図である。

#### 【0086】

この図7及び図8を用いてメディアユニークID（MID）の登録とコンテンツキーの取得動作を説明すると、まず、図7のフローチャートは、ユーザが前述のユーザ登録を正規に終了させることでスタートとなり、このメディアユニークID（MID）の登録及びコンテンツキーの取得行程がステップS11に進む。

#### 【0087】

ステップS11では、ユーザがインターネット5を介して自分のクライアント端末装置1をシステムサーバ装置4に接続する。これにより、このメディアユニークID（MID）の登録とコンテンツキーの取得行程がステップS12に進む。

#### 【0088】

なお、この例においては、前述のユーザ登録終了後に、クライアント端末装置1とシステムサーバ装置4との間で確立された通信回線を一端切断し、このメディアユニークID（MID）の登録とコンテンツキーの取得時に、再度、クライアント端末装置1とシステムサーバ装置4との間の通信回線を確立する説明とな

っているが、これは、前述のユーザ登録終了後に、クライアント端末装置1とシステムサーバ装置4との間で確立された通信回線を切断することなく、ユーザ登録に続けてこのメディアユニークID(MID)の登録とコンテンツキーの取得を行うようにしてもよい。この場合は、このメディアユニークID(MID)の登録及びコンテンツキーの取得行程は、スタートからステップS11をスキップしてステップS12に進むこととなる。

#### 【0089】

次にステップS12では、ユーザが、前述のように取得したユーザID(User ID)及びMC-IDと共に、これからダウンロードしようとするデジタルコンテンツが記憶された光ディスクに付された固有のIDであるメディアユニークID(MID)をシステムサーバ装置4側に送信する。これにより、このメディアユニークID(MID)の登録及びコンテンツキーの取得行程はステップS13に進む。

#### 【0090】

具体的には、CPU30は、メモリカード16と通信を行い、図8に示すようにMC-IDをシステムサーバ装置4側に送信し、前述のようにMC-Keyで暗号化されたユーザID(User ID)をメモリカード16から読み出してシステムサーバ装置4側に送信する。また、光ディスク制御部33により再生されたメディアユニークID(MID)をMC-Keyで暗号化し、これをシステムサーバ装置4側に送信する。

#### 【0091】

なお、この場合において、これらの各情報と共に、クライアントID及びHDD-IDをシステムサーバ装置4側に送信するようにしてもよい。この場合、クライアントID及びHDD-IDは、上記MC-IDと共にユーザが使用しているデバイスの特定に用いられるのであるが、MC-ID、クライアントID及びHDD-IDの3つのIDを用いてデバイスの特定を行うことで、MC-IDのみでデバイスの特定を行う場合よりも特定精度の向上を図ることができる。

#### 【0092】

また、クライアント端末装置1とシステムサーバ装置4との間においては、前

述のように例えばSSL (Secure Sockets Layer) 等の通信プロトコルに基づいて情報が暗号化されて送受信されるようになっており、通信の安全性が確保されている。

#### 【0093】

次に、ステップS13では、システムサーバ装置4が、クライアント端末装置1側から送信されたユーザID (User ID) が有効なIDであるか否かを判別する。そして、有効なユーザID (User ID) と判別された場合は、このメディアユニークID (MID) の登録及びコンテンツキーの取得行程がステップS14に進み、有効なユーザID (User ID) ではないと判別された場合は、このメディアユニークID (MID) の登録及びコンテンツキーの取得行程がステップS17に進む。

#### 【0094】

具体的には、システムサーバ装置4は、クライアント端末装置1側から送信されたMC-ID (及びクライアントID, HDD-ID) に基づいてユーザが使用しているデバイスを特定し、データベース3からこのMC-IDに対応するMC-Keyを読み出す。そして、このMC-Keyに基づいて、MC-Keyで暗号化されて送信されたユーザID (User ID) 及びメディアユニークID (MID) をそれぞれ復号化する。

#### 【0095】

前述のように、システムサーバ装置4側のデータベース3には、ユーザエントリ情報としてユーザID (User ID), MC-ID, クライアントID及びHDD-ID等が記憶されている。このため、システムサーバ装置4は、MC-ID (クライアントID及びHDD-ID) に基づいてデータベース3内のユーザ情報を検索し、このユーザ情報内のユーザID (User ID) と、現在システムサーバ装置4側にアクセスしてきているユーザのユーザID (User ID) とを照合する。そして両者が一致した場合には、現在システムサーバ装置4側にアクセスしてきているユーザは正規のユーザであると判断する。これにより、このメディアユニークID (MID) の登録及びコンテンツキーの取得行程がステップS14に進む。

## 【0096】

これに対して、システムサーバ装置4は、データベース3のユーザ情報内のユーザID（User ID）と、現在システムサーバ装置4側にアクセスしているユーザのユーザID（User ID）とが不一致の場合は無効なユーザID（User ID）と判別する。そして、ステップS17において、例えば「ユーザIDが無効です。ユーザ登録をして下さい。」等の再度のユーザ登録を促すメッセージをクライアント端末装置1側に返信する（無効通知）。これにより、中断されたかたちで、このメディアユニークID（MID）の登録及びコンテンツキーの取得行程が終了することとなる。

## 【0097】

次に、ステップS14では、システムサーバ装置4が、現在アクセスしているユーザの光ディスクから過去にHDD2へのダウンロードが行われたか否かを判別することで、その光ディスクに記録されているデジタルコンテンツがインストール済みであるか否かを判別する。

## 【0098】

具体的には、このダウンロードシステムにおいては、各光ディスクにそれぞれ付されたメディアユニークID（MID）は、システムサーバ装置4側のデータベース3に全て登録されている。そして、システムサーバ装置4は、デジタルコンテンツのダウンロードが行われた際に、データベース3のメディアユニークID（MID）に対してフラグを立てるようになっている。

## 【0099】

このため、システムサーバ装置4は、メディアユニークID（MID）を復号化すると、そのメディアユニークID（MID）に対してフラグが立っているか否かを検出することで、そのメディアユニークID（MID）を有する光ディスクから過去にデジタルコンテンツのダウンロードが行われたか否かを判別する。そして、そのメディアユニークID（MID）のフラグが立っていない場合、すなわちそのメディアユニークID（MID）が付された光ディスクから過去にデジタルコンテンツのダウンロードが行われていない場合には、データベース3内におけるそのメディアユニークID（MID）のフラグを立てると共に、このフ

ラグを立てたメディアユニークID（MID）をそのユーザのユーザエントリ情報に登録する。これにより、このメディアユニークID（MID）の登録及びコンテンツキーの取得行程がステップS15に進む。

#### 【0100】

これに対して、そのメディアユニークID（MID）のフラグが立っている場合、すなわちそのメディアユニークID（MID）が付された光ディスクから過去にデジタルコンテンツのダウンロードが行われている場合には、このメディアユニークID（MID）の登録及びコンテンツキーの取得行程がステップS17に進み、システムサーバ装置4が、例えば「このメディアからダウンロードはできません。」等のデジタルコンテンツのダウンロードを拒否するメッセージをクライアント端末装置1側に返信する（無効通知）。これにより、中断されたかたちで、このメディアユニークID（MID）の登録及びコンテンツキーの取得行程が終了することとなる。

#### 【0101】

次にステップS15では、そのユーザの光ディスクは、過去にデジタルコンテンツのダウンロードを行っていない光ディスクであるため、デジタルコンテンツのダウンロードを許可すべく、システムサーバ装置4が、そのユーザのメモリカード16に固有に付された暗号化鍵であるMC-Keyを用いて、その光ディスクに記録されているデジタルコンテンツを暗号化して記録する際に用いたコンテンツキー（Content-Key）を暗号化し、これをクライアント端末装置1側に送信する。

#### 【0102】

また、システムサーバ装置4は、ユーザエントリ情報からそのユーザが使用しているクライアント端末装置1のクライアントID及びHDD2のHDD-IDを読み出し、これら各IDを、例えば乱数を用いて形成した「コンテンツジェンキー（Content-Gen-Key）」で暗号化してクライアント端末装置1側に返信すると共に、コンテンツジェンキー（Content-Gen-Key）をMC-Keyで暗号化してクライアント端末装置1側に返信する。

#### 【0103】

すなわち、この例の場合、システムサーバ装置4は、ダウンロードを行うデジタルコンテンツを復号化するためのコンテンツキー（Content-Key）をMC-Keyで暗号化してクライアント端末装置1側に返信すると共に、デジタルコンテンツのダウンロードが可能なデバイスを予め登録されているそのユーザーのクライアント端末装置1及びHDD2に制限するためにコンテンツジェンキー（Content-Gen-Key）で暗号化したクライアントID及びHDD-IDをクライアント端末装置1側に返信している。また、コンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDを復号化するためのコンテンツジェンキー（Content-Gen-Key）をMC-Keyで暗号化してクライアント端末装置1側に返信している。

#### 【0104】

次に、ステップS16では、クライアント端末装置1が、システムサーバ装置4側から返信されたMC-Keyで暗号化されたコンテンツキー（Content-Key）、MC-Keyで暗号化されたコンテンツジェンキー（Content-Gen-Key）、及びコンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDをそれぞれメモリカード16に記憶制御する。これにより、この図7のフローチャートに示すメディアユニークIDの登録とコンテンツキーの取得の全行程が終了する。

#### 【0105】

このように、このダウンロードシステムにおいては、HDD2へのダウンロードを行う際には、ダウンロードを許可する前に、メディアユニークID（MID）の照合が行われ、過去にダウンロードの履歴のない光ディスクに対してのみデジタルコンテンツのダウンロードが許可されるようになっている。このため、光ディスクからのデジタルコンテンツのダウンロードを1回に制限することができ、同じ光ディスクから多数の他のユーザーのHDD2にデジタルコンテンツがダウンロードされる不正使用を防止することができる。

#### 【0106】

（デジタルコンテンツのダウンロード）

次に、このようにしてコンテンツキー（Content-Key）を取得すると、光ディスクに記録されているデジタルコンテンツをHDD2にダウンロードすることが可能となる。

#### 【0107】

図9はこのダウンロード行程の流れを示すフローチャート、図10はこのダウンロードを行う際にクライアント端末装置1、HDD2及びメモリカード16の間で取り扱う情報を模式的に示した図である。この図9及び図10を用いてデジタルコンテンツのダウンロード行程を説明すると、まず、図9のフローチャートは、ユーザが前述のメディアユニークIDの登録及びコンテンツキーの取得を正規に終了させ、デジタルコンテンツのダウンロードを指定することでスタートとなり、このダウンロード行程がステップS21に進む。

#### 【0108】

ステップS21では、クライアント端末装置1のIOP32が、それぞれMC-Keyで暗号化されたコンテンツキー（Content-Key）及びコンテンツジェンキー（Content-Gen-Key）をメモリカード16から読み出し、これらをCPU30に供給する。

#### 【0109】

前述のように、MC-Keyは、システムサーバ装置4側及びこのクライアント端末装置1でそれぞれ保持している。このため、CPU30は、このMC-Keyで暗号化されたコンテンツキー（Content-Key）及びコンテンツジェンキー（Content-Gen-Key）を、保持しているMC-Keyを用いて復号化処理し、この復号化されたコンテンツキー（Content-Key）及びコンテンツジェンキー（Content-Gen-Key）をRAM36に記憶制御する。これにより、このダウンロード行程がステップS22に進む。

#### 【0110】

ステップS22では、IOP32が、コンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDをメモリカード16から読み出し、これらをCPU30に供給する。CPU30は、先に

復号化したコンテンツジェンキー（Content-Gen-Key）を用いてこのクライアントID及びHDD-IDを復号化する。

#### 【0111】

そして、CPU30が、このクライアント端末装置1に付されたクライアントID及びこのクライアント端末装置1に接続されているHDD2に付されたHDD-IDを、メモリカード16から読み出されコンテンツジェンキー（Content-Gen-Key）で復号化されたクライアントID及びHDD-IDと照合する。これにより、このダウンロード行程がステップS23に進む。

#### 【0112】

ステップS23では、CPU30が、メモリカード16から復号化されたクライアントID及びHDD-IDは、そのクライアント端末装置1のクライアントID及びHDD2のHDD-IDと一致するか否か（クライアントID及びHDD-IDは正しいか否か）を判別する。両者が一致する場合はデジタルコンテンツのダウンロードを行うべくこのダウンロード行程がステップS24に進み、両者が不一致の場合はこのダウンロード行程がステップS28に進む。

#### 【0113】

メモリカード16から復号化されたクライアントID及びHDD-IDが、そのクライアント端末装置1のクライアントID及びHDD-IDと一致しないということは、前述のコンテンツキー（Content-Key）の取得が、そのクライアント端末装置1及びHDD2に基づいて行われていないことを示す。すなわち、メモリカード16だけ第3者から借りてきてデジタルコンテンツのダウンロードを行おうとしていることを示している。

#### 【0114】

このため、CPU30は、例えば「このメモリカードではダウンロードを行うことはできません。」等のダウンロードを拒否するメッセージをユーザに対して表示制御する。これにより、中断されたかたちでこのダウンロード行程が終了することとなる。

#### 【0115】

これに対してステップS24では、メモリカード16から復号化されたクライ

アントID及びHDD-IDが、そのクライアント端末装置1のクライアントID及びHDD-IDと一致したため、CPU30が、光ディスク制御部33により再生された光ディスクからのデジタルコンテンツを、RAM36に記憶されているコンテンツキー(Content-Key)を用いて復号化すると共に、この復号化したデジタルコンテンツを、RAM36に記憶されているコンテンツジェンキー(Content-Gen-Key)で再暗号化してHDD2に供給する。これにより、このダウンロード行程がステップS25に進む。

#### 【0116】

次に、ステップS25では、HDD2が、クライアント端末装置1側から供給されたコンテンツジェンキー(Content-Gen-Key)で再暗号化されたデジタルコンテンツを保存する。これにより、図10に示すようにコンテンツジェンキー(Content-Gen-Key)で再暗号化されたデジタルコンテンツがHDD2に記憶され、このダウンロード行程がステップS26に進む。

#### 【0117】

次に、ステップS26ではクライアント端末装置1のCPU30がHDD2と通信を行うことで、デジタルコンテンツのダウンロードが完了したか否かを判別し、ダウンロードが完了していない場合は、前述のステップS24及びステップS25の動作を繰り返し実行することで、デジタルコンテンツのダウンロードが完了するまでHDD2にデジタルコンテンツの供給を行う。そして、ダウンロードが完了したタイミングで、このダウンロード行程がステップS27に進む。

#### 【0118】

ステップS27では、デジタルコンテンツのダウンロードが完了したため、IOP32が、メモリカード16に記憶されているコンテンツキー(Content-Key)を消去する。これにより、このダウンロード行程の全行程が終了する。

#### 【0119】

前述のように、光ディスクに記録されているデジタルコンテンツは、コンテンツキー(Content-Key)で暗号化されているため、このデジタルコン

コンテンツをHDD2にダウンロードするには、コンテンツキー（Content-Key）で復号化してダウンロードする必要があるのであるが、一端ダウンロードシステムが終了した後は、メモリカード16内のコンテンツキー（Content-Key）を消去することにより、コンテンツキー（Content-Key）を再度取得することはできないため、デジタルコンテンツの再度のダウンロードを防止することができ、デジタルコンテンツのダウンロードを1回に制限してデジタルコンテンツの不正使用を防止することができる。

## 【0120】

（HDDにダウンロードされたデジタルコンテンツの再生）

次に、このようにHDD2にダウンロードされたデジタルコンテンツは、ユーザが繰り返し再生して利用するようになっている。

## 【0121】

図11に、HDD2に保存されたデジタルコンテンツの再生行程の流れを示すフローチャートを、図12にこの再生行程において、クライアント端末装置1、HDD2及びメモリカード16の間で取り扱われる情報を模式的に示した図を示す。この図11及び図12を用いてデジタルコンテンツの再生行程を説明すると、まず、図11のフローチャートは、ユーザが前述のデジタルコンテンツのダウンロードを正規に終了させ、デジタルコンテンツの再生を指定することでスタートとなり、このデジタルコンテンツの再生行程がステップS31に進む。

## 【0122】

ステップS31では、クライアント端末装置1のIOP32が、メモリカード16に記憶されているMC-Keyで暗号化されて記憶されたコンテンツジェンキー（Content-Gen-Key）を読み出し、これをCPU30に供給する。CPU30は、このMC-Keyで暗号化されたコンテンツジェンキー（Content-Gen-Key）を、クライアント端末装置1側で保持しているMC-Keyを用いて復号化しコンテンツジェンキー（Content-Gen-Key）を再生する。これにより、このデジタルコンテンツの再生行程がステップS32に進む。

## 【0123】

ステップS32では、IOP32が、コンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDをメモリカード16から読み出し、これをCPU30に供給する。CPU30は、先に復号化したコンテンツジェンキー（Content-Gen-Key）を用いて、この暗号化されたクライアントID及びHDD-IDを復号化する。これにより、このデジタルコンテンツの再生行程がステップS33に進む。

#### 【0124】

ステップS33では、CPU30が、クライアント端末装置1に付されているクライアントID及びHDD2に付されているHDD-IDと、コンテンツジェンキー（Content-Gen-Key）で復号化したクライアントID及びHDD-IDとを照合する。そして、両者が一致しない場合は、他のユーザのメモリカード16、他のユーザのクライアント端末装置1、或いは他のユーザのHDD2が用いられていることを示すため、CPU30がステップS35において、例えば「デジタルコンテンツを再生することはできません。」等のデジタルコンテンツの再生を拒否するメッセージをユーザに表示する。これにより、中断されるかたちでこのデジタルコンテンツの再生行程が終了することとなる。

#### 【0125】

このように、このダウンロードシステムにおいては、HDD2にダウンロードされたデジタルコンテンツを再生する際にも、クライアントID及びHDD-IDの照合を行うようになっているため、メモリカード16とデジタルコンテンツが保存されたHDD2を他のユーザに貸与した場合でも、クライアントID及びHDD-IDが一致しないため、そのHDD2に保存されているデジタルコンテンツは再生することはできない。このため、HDD2にダウンロードされたデジタルコンテンツの不正使用を強力に防止することができる。

#### 【0126】

次に、クライアント端末装置1に付されているクライアントID及びHDD2に付されているHDD-IDと、コンテンツジェンキー（Content-Gen-Key）で復号化したクライアントID及びHDD-IDとが一致した場合には、正規のユーザからの再生指示であるため、CPU30は、先に復号化した

コンテンツジェンキー（Content-Gen-Key）を用いて、コンテンツジェンキー（Content-Gen-Key）で暗号化されているHDD2のデジタルコンテンツを復号化し、これをRAM36に記憶する。これにより、このデジタルコンテンツの再生の全行程が終了する。

#### 【0127】

RAM36に記憶されたデジタルコンテンツが、例えばビデオゲームのゲームプログラムであった場合には、CPU30がこのゲームプログラムに基づいて動作し、ビデオゲームのキャラクタを表示制御し、効果音やBGM等を発音制御する。これにより、ユーザは光ディスクからHDD2にダウンロードしたゲームプログラムに基づいてビデオゲームを楽しむことができる。

#### 【0128】

光ディスクからゲームプログラムを直接再生してビデオゲームを行うようになると、新たなビデオゲームを行う毎に光ディスクの着脱作業が必要なのであるが、このように各光ディスクに記録されたゲームプログラムをHDD2に保存しておくことにより、新たなビデオゲームを行う毎に必要となっていた光ディスクの着脱作業を省略することができ、新たなビデオゲームをスムーズに開始可能とすることができる。

#### 【0129】

なお、前述のように光ディスクからデジタルコンテンツのダウンロードが終了した後には、メモリカード16に記憶されているコンテンツキー（Content-Key）が消去され、再度のダウンロードは行えないようになっているのであるが、メモリカード16に記憶されているコンテンツジェンキー（Content-Gen-Key）はダウンロード完了後も消去されないため、コンテンツジェンキー（Content-Gen-Key）で暗号化されて保存されたデジタルコンテンツは、このメモリカード16に記憶されているコンテンツジェンキー（Content-Gen-Key）を用いて繰り返し復号化して再生可能である。

#### 【0130】

（デバイスの修理、交換に対する対応）

次に、このダウンロードシステムにおいては、前述のようにシステムサーバ装置4側でクライアントID, HDD-ID, MC-ID, ユーザID（User ID）の組み合わせをユーザエントリ情報として一括して管理するようになっているため、クライアント端末装置1やHDD2を破損等により交換した場合、この交換したクライアント端末装置1やHDD2のクライアントIDやHDD-IDが、ユーザエントリ情報として登録されているクライアントIDやHDD-IDと異なるものとなり、以後、正規なユーザであるにも拘わらずデジタルコンテンツのダウンロードや再生を行うことができなくなる不都合を生ずる。

#### 【0131】

ただ、このダウンロードシステムの場合、クライアントIDやHDD-ID等のIDの固有性を確保することでデジタルコンテンツの不正使用を防止するようになっているため、そのデバイスが故障し、例え修理でそのデバイスが正常に動作するようになったとしても、この修理後のデバイスに対して故障前に付与されたクライアントIDやHDD-IDとは異なるクライアントIDやHDD-IDを新たに付与してIDの固有性を確保し、デジタルコンテンツの不正使用を防止することが好ましい。このため、このダウンロードシステムでは、デバイスを修理或いは交換した場合には、そのデバイスに対して新たなIDを改め付与することで、IDの固有性を確保するようになっている。

#### 【0132】

（クライアント端末装置及びHDDの修理、交換に対する対応）

図13に、このダウンロードシステムにおけるクライアント端末装置及びHDDの修理、交換に対する対応を説明するための模式図を示す。この図13中、×印が描かれているクライアント端末装置1或いはHDD2は、破損したクライアント端末装置1或いはHDD2を示している。

#### 【0133】

この図13において、クライアント端末装置1或いはHDD2が破損した場合、ユーザは、その破損したクライアント端末装置1或いはHDD2を、メモリカード16と共に、このダウンロードシステムを管理する管理者側のリペアセンター等に送付する。

## 【0134】

すなわち、この場合メモリカード16は破損していないのであるが、メモリカード16にはコンテンツジェンキー（Content-Gen-Key）やコンテンツジェンキー（Content-Gen-Key）で暗号化されたクライアントID及びHDD-IDが記憶されているため、クライアント端末装置1或いはHDD2が破損した場合でも、この破損したクライアント端末装置1或いはHDD2と共にメモリカード16を上記リペアセンター等に送付（或いは持ち込み）するようになっている。

## 【0135】

リペアセンターでは、故障したクライアント端末装置1或いはHDD2が送付されると、このクライアント端末装置1或いはHDD2が正常に動作するように修理、交換等すると共に、この修理、交換等したクライアント端末装置1或いはHDD2に対して新たなクライアントID或いはHDD-IDを付与する。

## 【0136】

具体的には、クライアント端末装置1のクライアントIDは、例えば上記デバイスIDやオペレーティングシステムプログラムと共にMASK-ROM35に記憶されている。また、HDD2内にも上記MASK-ROM35と同様のMASK-ROMが設けられており、HDD-IDは、このMASK-ROMに記憶されている。このため、リペアセンターでは、装置の修理を行った場合には、この修理を行う前に設けられていたMASK-ROMを取り外し、新たなクライアントID或いはHDD-IDが記憶されたMASK-ROMに交換することで、新たなクライアントID或いはHDD-IDの付与を行う。

## 【0137】

なお、装置の修理を行った場合には、前に付与されていたクライアントID或いはHDD-IDが記憶されたMASK-ROMが装置内に存在するため、このような新たなクライアントID或いはHDD-IDが記憶されたMASK-ROMに交換する作業を行うのであるが、装置自体を新品の装置に交換する場合は、この新品の装置に、故障した装置とは異なるクライアントID或いはHDD-IDが付与されているため、上記MASK-ROMの交換は行わない。

## 【0138】

次に、リペアセンターでは、故障したクライアント端末装置1或いはHDD2と共に送付されたメモリカード16のMC-IDを再生し、このMC-IDからクライアント端末装置1のデータベース3に記憶されているユーザエントリ情報を参照し、ユーザ側においてそのメモリカード16を用いてHDD2にダウンロードされたデジタルコンテンツを検出し、システムサーバ装置4のデータベース3のユーザエントリ情報のクライアントID及びHDD-IDを、新たに付与したクライアントID及びHDD-IDに記録し直す。

## 【0139】

また、メモリカード16に記録されているMC-Keyで暗号化されたコンテンツジェンキー(Content-Key)と、コンテンツジェンキー(Content-Key)で暗号化されたクライアントID及びHDD-IDとをそれぞれ消去する。そして、このメモリカード16を、修理、交換等したクライアント端末装置1或いはHDD2と共にユーザ側に返送する。

## 【0140】

これにより、ユーザ側のデバイス(クライアント端末装置1、HDD2及びメモリカード16)は、図5及び図6を用いて説明した前述のユーザ登録行程が終了した直後の状態に戻ることとなる。

## 【0141】

このメモリカード16及びクライアント端末装置1或いはHDD2が返送されたユーザは、図7及び図8を用いて説明したメディアユニークID(MID)の登録とコンテンツキー(Content-Key)を再度取得し、このコンテンツキー(Content-Key)を用いてデジタルコンテンツのダウンロードを再度行う。

## 【0142】

前述のように、新たなクライアントIDやHDD-IDが付与された場合でも、システムサーバ装置4側で、この新たに付与したクライアントIDやHDD-IDに応じてデータベース3のユーザエントリ情報を書き換えていたため、コンテンツキー(Content-Key)の取得時やデジタルコンテンツのダウ

ロード時に、新たなクライアントIDやHDD-IDをそのまま用いて再ダウンロードを行うことができる。

#### 【0143】

(メモリカードの破損、紛失に対する対応)

次に、以上の説明は、クライアント端末装置1或いはHDD2の修理、交換に対する対応であったが、メモリカード16が破損し或いは紛失した場合、このダウンロードシステムにおいては、以下に説明するように対応するようになっている。図14に、このダウンロードシステムにおけるメモリカード16の破損、紛失に対する対応を説明するための模式図を示す。この図14中、点線の枠で囲んで示すメモリカード16が、破損或いは紛失したメモリカード16を示している。

#### 【0144】

この図14において、メモリカード16が破損或いは紛失した場合、ユーザは、インターネット5を介してクライアント端末装置1をシステムサーバ装置4に接続し、システムサーバ装置4に対してメモリカードの再発行を申請する。

#### 【0145】

この申請がなされるとシステムサーバ装置4は、ユーザID(User ID)の入力画面の情報をクライアント端末装置1側に送信する。ユーザは、クライアント端末装置1によりテレビジョン受像機18に表示される入力画面に対して、先に取得したユーザID(User ID)を入力しシステムサーバ装置4側に返信する。

#### 【0146】

なお、この場合、メモリカード16が破損或いは紛失した場合なので、メモリカード16からユーザID(User ID)を読み出すことはできない。このため、ユーザはメモリカード16の破損或いは紛失に備えて、ユーザID(User ID)が発行された際にこれをメモ帳等に書き写しておくことが好ましいであろう。

#### 【0147】

次にシステムサーバ装置4は、このユーザから返信されたユーザID(User

r ID) を受信すると、データベース3に記憶されているこのユーザID (User ID) に対応するユーザエントリ情報を参照する。これにより、システムサーバ装置4側では、破損或いは紛失したメモリカード16のMC-ID及びMC-Keyと共に、コンテンツジェンキー (Content-Gen-Key) やそのメモリカード16でダウンロードされたデジタルコンテンツ等を知ることができる。

#### 【0148】

このため、システムサーバ装置4は、新たなMC-IDを有するメモリカード16newを用意し、このメモリカード16newに新たなMC-Key (New-MC-Key) と、このNew-MC-Keyで新たに暗号化したコンテンツジェンキー (Content-Gen-Key) と、このコンテンツジェンキー (Content-Gen-Key) で暗号化したクライアントID及びHDD-IDを記録し直すと共に、データベース3に記憶されているユーザエントリ情報が、この新たなメモリカード16Newに対応したユーザエントリ情報となるように、MC-IDやMC-Key等の書き換えを行う。

#### 【0149】

なお、この場合、メモリカード16が破損或いは紛失した場合であり、ユーザのクライアント端末装置1及びHDD2は正常に動作している。このため、コンテンツジェンキー (Content-Gen-Key) で暗号化されるクライアントID及びHDD-IDは、元のIDをそのまま用いて暗号化を施すようになっている。

#### 【0150】

リペアセンター側では、このメモリカード16newを、例えば郵送等によりユーザ側に物理的に送付する。前述のように、システムサーバ装置4側ではこのメモリカード16new内の各情報の書き換えと共に、データベース3のユーザエントリ情報の書き換えを行っている。このため、送付されたメモリカード16newを受け取ったユーザは、このメモリカード16new、クライアント端末装置1及びHDD2の組み合わせのシステムを用いて、以前と同様に、デジタルコンテンツのダウンロードやダウンロードしたデジタルコンテンツの再生等を行

うことができる。

### 【0151】

#### [第1の実施の形態の効果]

以上の説明から明らかなように、この第1の実施の形態のダウンロードシステムは、ユーザが使用しているクライアント端末装置1、HDD2及びメモリカード16に固有のIDであるクライアントID、HDD-ID及びMC-IDをそれぞれ付し、この各IDの組み合わせのシステム以外ではデジタルコンテンツのHDD2へのダウンロードを禁止すると共に、デジタルコンテンツをダウンロードする際には、光ディスク毎に付されている固有のIDであるメディアユニークID（MID）の登録を条件にデジタルコンテンツのダウンロードを許可するようになっている。

### 【0152】

このため、デジタルコンテンツのHDD2へのダウンロードを、正当なユーザに限定し、ダウンロード可能回数を1回に制限して可能とすることができます。このため、他のユーザは貸与された光ディスクからのデジタルコンテンツのダウンロードは行うことができず、1枚の光ディスクのデジタルコンテンツが、他のユーザのHDD2に次々と不正にダウンロードされてしまうような不都合を防止することができる。

### 【0153】

#### [第2の実施の形態]

次に本発明の第2の実施の形態となるダウンロードシステムの説明をする。上述の第1の実施の形態のダウンロードシステムは、ユーザが自分のクライアント端末装置1をシステム管理者側のシステムサーバ装置4に直接的に接続してユーザ登録を行い、コンテンツキー（Content-Key）等を取得してデジタルコンテンツのダウンロードを行うものであったが、この第2の実施の形態のダウンロードシステムは、ユーザのクライアント端末装置1とシステム管理者側のシステムサーバ装置4との間に、第3者が管理する第3者管理サーバ装置を設け、ユーザはこの第3者管理サーバ装置を介してコンテンツキー（Content-Key）等の取得を行い、第3者管理サーバ装置側ではこのコンテンツキー（

Content-Key) 等の提供に対する課金を行うようにしたものである。

#### 【0154】

##### (第2の実施の形態の構成)

図15に、この第2の実施の形態となるダウンロードシステムのシステム構成図を示す。この図15は、光ディスクからデジタルコンテンツをダウンロードする際にコンテンツキー (Content-Key) を取得する流れを示している。同様の流れを示す図8とこの図15を比較して、クライアント端末装置1とシステムサーバ装置4との間に第3者管理サーバ装置50が設けられているのが理解できるであろう。

#### 【0155】

この図15において、システムサーバ装置4と第3者管理サーバ装置50とは、例えば専用回線や、公衆回線を専用回線のように利用可能なVPN (Virtual Private Network) 等により相互に接続されている。

#### 【0156】

また、システムサーバ装置4はインターネット5には接続されておらず、この第3者管理サーバ装置50がインターネット5に接続されている。このため、ユーザは、システムサーバ装置4に対して直接的にアクセスすることはできず、この第3者管理サーバ装置50を介して間接的にシステムサーバ装置4にアクセスすることとなる。

#### 【0157】

##### (第2の実施の形態の動作)

次に、この第2の実施の形態のダウンロードシステムの動作説明をする。この第2の実施の形態のダウンロードシステムの場合、光ディスクからデジタルコンテンツのダウンロードを行おうとするユーザは、インターネット5を介して自分のクライアント端末装置1を第3者管理サーバ装置50に接続し、MC-ID, ユーザID (User ID), メディアユニークID (MID) と共に、第3者管理サーバ装置50用のアカウント情報（例えばユーザ名やパスワード等）を第3者管理サーバ装置50側に送信する。

#### 【0158】

クライアント端末装置1は、MC-ID及びアカウント情報をそのまま第3者管理サーバ装置50側に送信すると共に、ユーザID(User ID)及び光ディスクのメディアユニークID(MID)をMC-Keyで暗号化し、これらを第3者管理サーバ装置50側に送信する。

#### 【0159】

第3者管理サーバ装置50は、クライアント端末装置1側から送信された各情報のうち、アカウント情報を抽出して取得すると共に、専用回線（或いは上記VPN）を介してMC-ID, MC-Keyで暗号化されたユーザID(User ID)及びMC-Keyで暗号化されたメディアユニークID(MID)をシステムサーバ装置4側に送信する。

#### 【0160】

システムサーバ装置4は、このMC-ID, MC-Keyで暗号化されたユーザID(User ID)及びMC-Keyで暗号化されたメディアユニークID(MID)を受信すると、前述と同様に暗号化されて光ディスクに記録されているデジタルコンテンツを復号化するためのコンテンツキー(Content-Key)をMC-Keyで暗号化し、また、コンテンツジェンキー(Content-Gen-Key)をMC-Keyで暗号化し、さらにこのコンテンツジェンキー(Content-Gen-Key)でユーザのクライアントID及びHDD-IDを暗号化して第3者管理サーバ装置50に返信する。

#### 【0161】

第3者管理サーバ装置50は、このMC-Keyで暗号化されたコンテンツキー(Content-Key), MC-Keyで暗号化されたコンテンツジェンキー(Content-Gen-Key)、及びコンテンツジェンキー(Content-Gen-Key)で暗号化されたユーザのクライアントID, HDD-IDを、それぞれインターネット5を介してユーザのクライアント端末装置1に転送する。そして、この転送の際に、コンテンツキー(Content-Key)を提供した代償として、クライアント端末装置1が第3者管理サーバ装置50にアクセスする際にクライアント端末装置1から送信された第3者管理サーバ装置50用のアカウント情報に基づいて、そのユーザに対する課金を行う。

## 【0162】

クライアント端末装置1は、このMC-Keyで暗号化されたコンテンツキー(Content-Key)、MC-Keyで暗号化されたコンテンツジェンキー(Content-Gen-Key)、及びコンテンツジェンキー(Content-Gen-Key)で暗号化されたユーザのクライアントID、HDD-IDを受信すると、これらをメモリカード16に記憶制御して、前述のようにデジタルコンテンツのダウンロード、及びダウンロードしたデジタルコンテンツの再生に用いる。

## 【0163】

また、第3者管理サーバ装置50側には、例えばユーザのクレジットカードの番号や、プリペイドされた金額情報が予め登録されている。このため、第3者管理サーバ装置50は、コンテンツキー(Content-Key)の提供と引き替えに課金した金額を、このクレジットカード会社に請求して回収し、或いはプリペイドされている残金から課金分の金額を減算して回収する。そして、この回収した金銭を、システムサーバ装置4の管理者側と第3者管理サーバ装置50の管理者側との間で、所定の割合で分配する。

## 【0164】

## [第2の実施の形態の効果]

このようにこの第2の実施の形態のダウンロードシステムは、クライアント端末装置1とシステムサーバ装置4との間に第3者管理サーバ装置50を設けて構成し、ユーザはこの第3者管理サーバ装置50を介してシステムサーバ装置4にアクセスしてコンテンツキー(Content-Key)の配布を請求し、第3者管理サーバ装置50は、このコンテンツキー(Content-Key)をユーザに配布した際に課金を行う。

## 【0165】

これにより、第3者(第3者管理サーバ装置50の管理者)が介在した状態でのダウンロードシステムを構築することができ、ひとつのネットビジネスを形成することができる他、上述の第1の実施の形態のダウンロードシステムと同じ効果を得ることができる。

【0166】

また、コンテンツキー（Content-Key）をユーザに配布した際に課金を行うようになっているため、光ディスク自体を無償でユーザに対して配布することを可能とすることができます。

【0167】

また、このように光ディスク自体を無償でユーザに対して配布し、コンテンツキー（Content-Key）をユーザに配布した際に課金を行うようにすることで、光ディスクに付すメディアユニークID（MID）を不要とすることができる（光ディスクに対してMIDを付す必要がない。）。

【0168】

すなわち、光ディスクに対してMIDを付すことなくユーザに配布し、ユーザからダウンロードの申請があった際に、システムサーバ装置4或いは第3者管理サーバ装置50が、そのユーザに対して、コンテンツの復号化のためのコンテンツキー（Content-Key）を配布すると共に課金を行うようにしてもよい。

【0169】

なお、この第2の実施の形態の例では、第3者管理サーバ装置50側において課金を行うこととしたが、これは、システムサーバ装置4側で課金を行うようにしてもよい。

【0170】

最後に、本発明は一例として説明した上述の実施の形態に限定されることはない。このため、上述の実施の形態以外であっても、本発明に係る技術的思想を逸脱しない範囲であれば、設計等に応じて種々の変更が可能であることは勿論であることを付け加えておく。

【0171】

【発明の効果】

本発明は、記憶媒体に記憶されたコンテンツをダウンロード機器を用いてダウンロードする場合に、記憶媒体の持ち主である正規のユーザにのみ、このダウンロードを許可することができる。このため、他のユーザは、同じ記憶媒体から他

のユーザが所有する第2の記憶媒体にコンテンツをダウンロードすることはできず、記憶媒体に記憶されたコンテンツの不正使用を防止することができる。

【図面の簡単な説明】

【図1】

本発明の第1の実施の形態のダウンロードシステムのシステム構成を示すブロック図である。

【図2】

ダウンロードシステムを構成するクライアント端末装置及びハードディスクドライブ（HDD）の外観を示す斜視図である。

【図3】

クライアント端末装置の電気的な構成を示すブロック図である。

【図4】

コンテンツキー（Content-Key）で暗号化されたデジタルコンテンツが記憶された、このダウンロードシステムに用いられる光ディスクを説明するための図である。

【図5】

ダウンロードシステムにおけるユーザ登録の流れを示すフローチャートである

【図6】

ユーザ登録時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すダウンロードシステムの模式図である。

【図7】

ダウンロードシステムにおける、光ディスクに個別に付されたメディアユニークID（MID）の登録動作と、コンテンツキー（Content-Key）の取得動作を示すフローチャートである。

【図8】

光ディスクに個別に付されたメディアユニークID（MID）の登録時、及びコンテンツキー（Content-Key）の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示すダウンロードシステムの

模式図である。

【図9】

ダウンロードシステムにおけるダウンロード実行時の流れを示すフローチャートである。

【図10】

ダウンロード実行時にクライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される各情報を示す模式図である。

【図11】

ダウンロードシステムにおける、ハードディスクドライブにダウンロードしたデジタルコンテンツの再生動作を示すフローチャートである。

【図12】

ハードディスクドライブにダウンロードしたデジタルコンテンツの再生時に、クライアント端末装置、メモリカード及びハードディスクドライブの間で送受信される情報を示す模式図である。

【図13】

クライアント端末装置或いはハードディスクドライブの修理或いは交換に対するダウンロードシステムの対応を説明するための模式図である。

【図14】

メモリカードの破損或いは紛失に対するダウンロードシステムの対応を説明するための模式図である。

【図15】

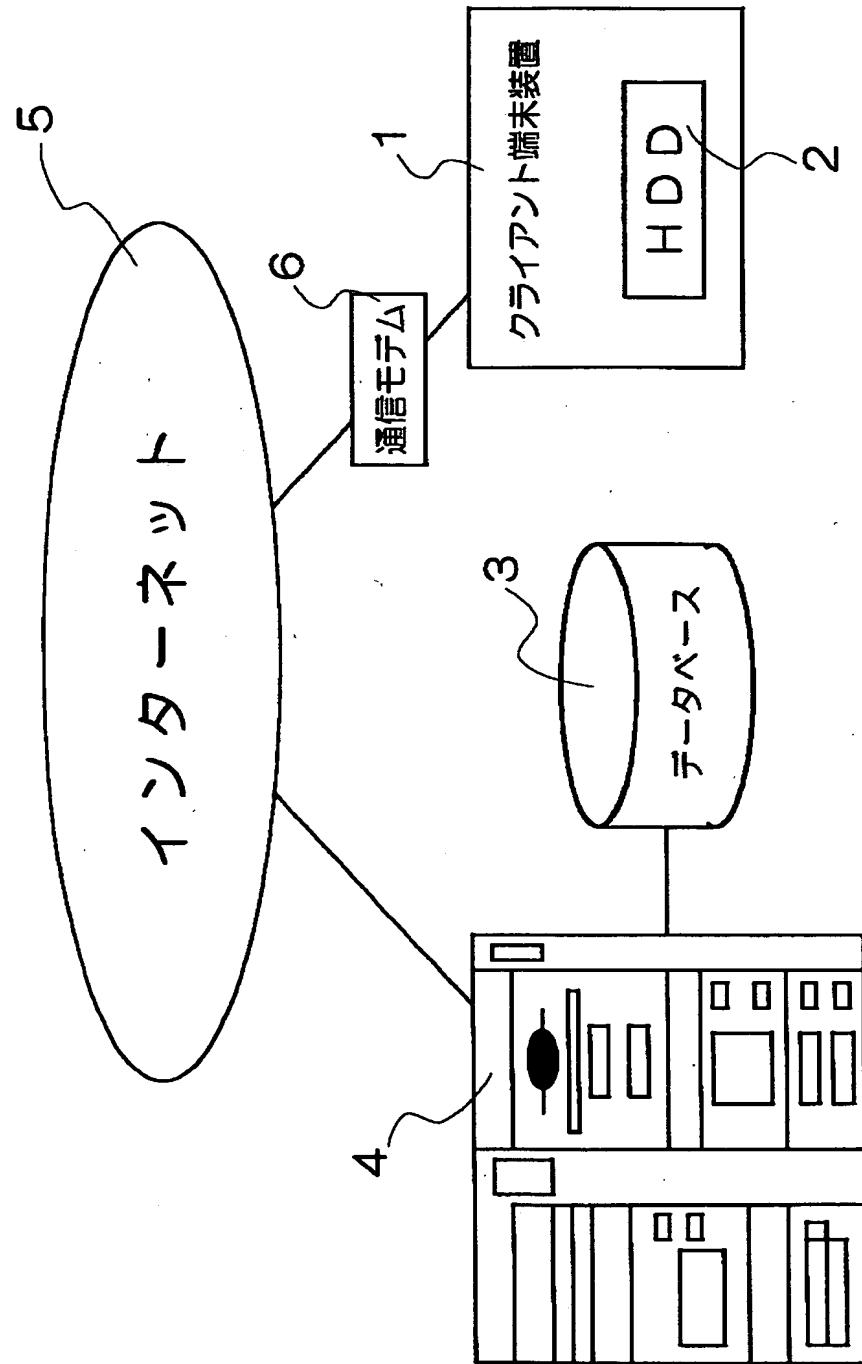
光ディスクに個別に付されたメディアユニークID (MID) の登録時、及びコンテンツキー (Content-Key) の取得時にクライアント端末装置とシステムサーバ装置との間で送受信される各情報を示す、本発明の第2の実施の形態となるダウンロードシステムの模式図である。

【符号の説明】

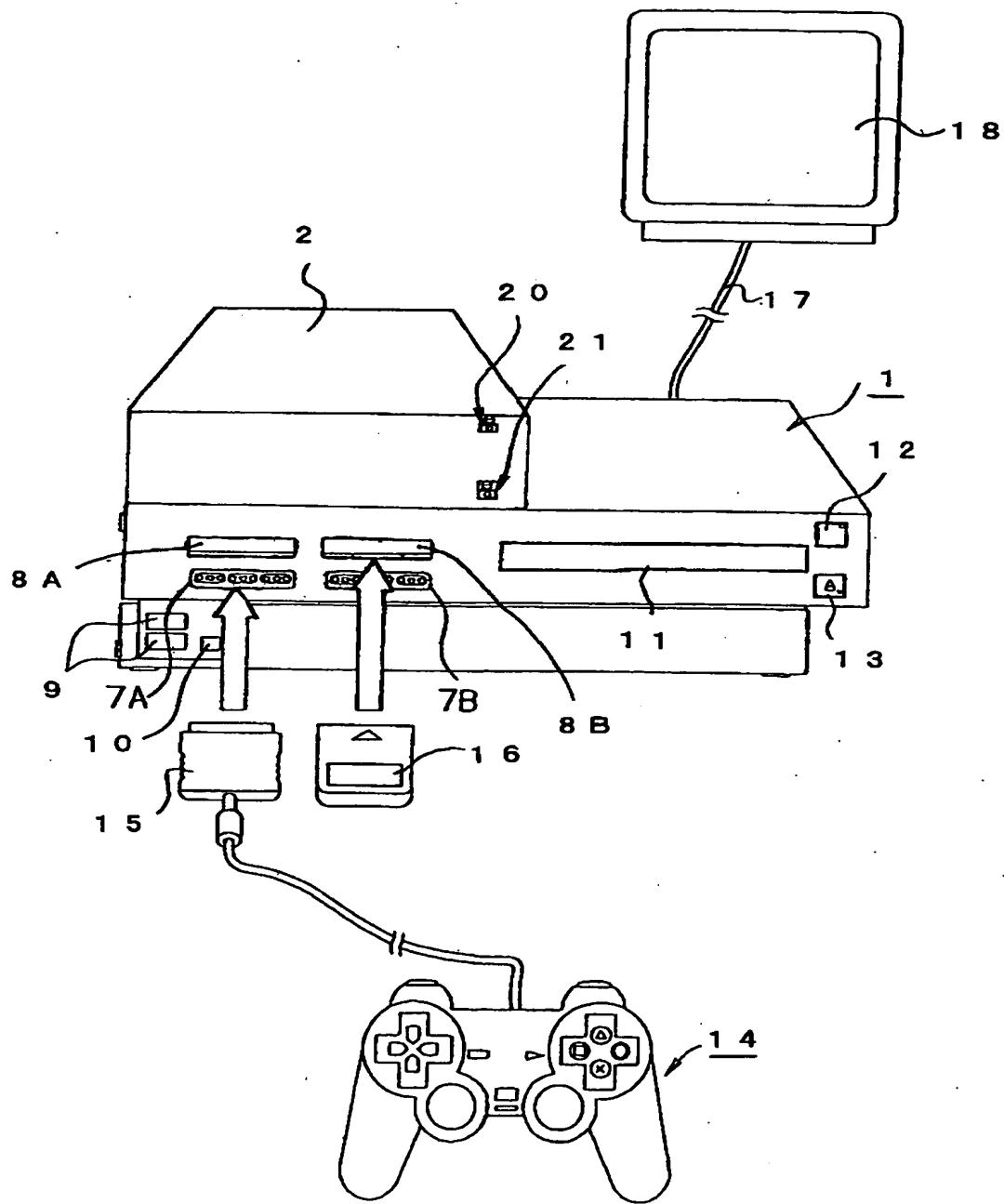
1…クライアント端末装置、2…ハードディスクドライブ (HDD)、3…データベース、4…システムサーバ装置、5…インターネット、6…通信モデム

【書類名】 図面

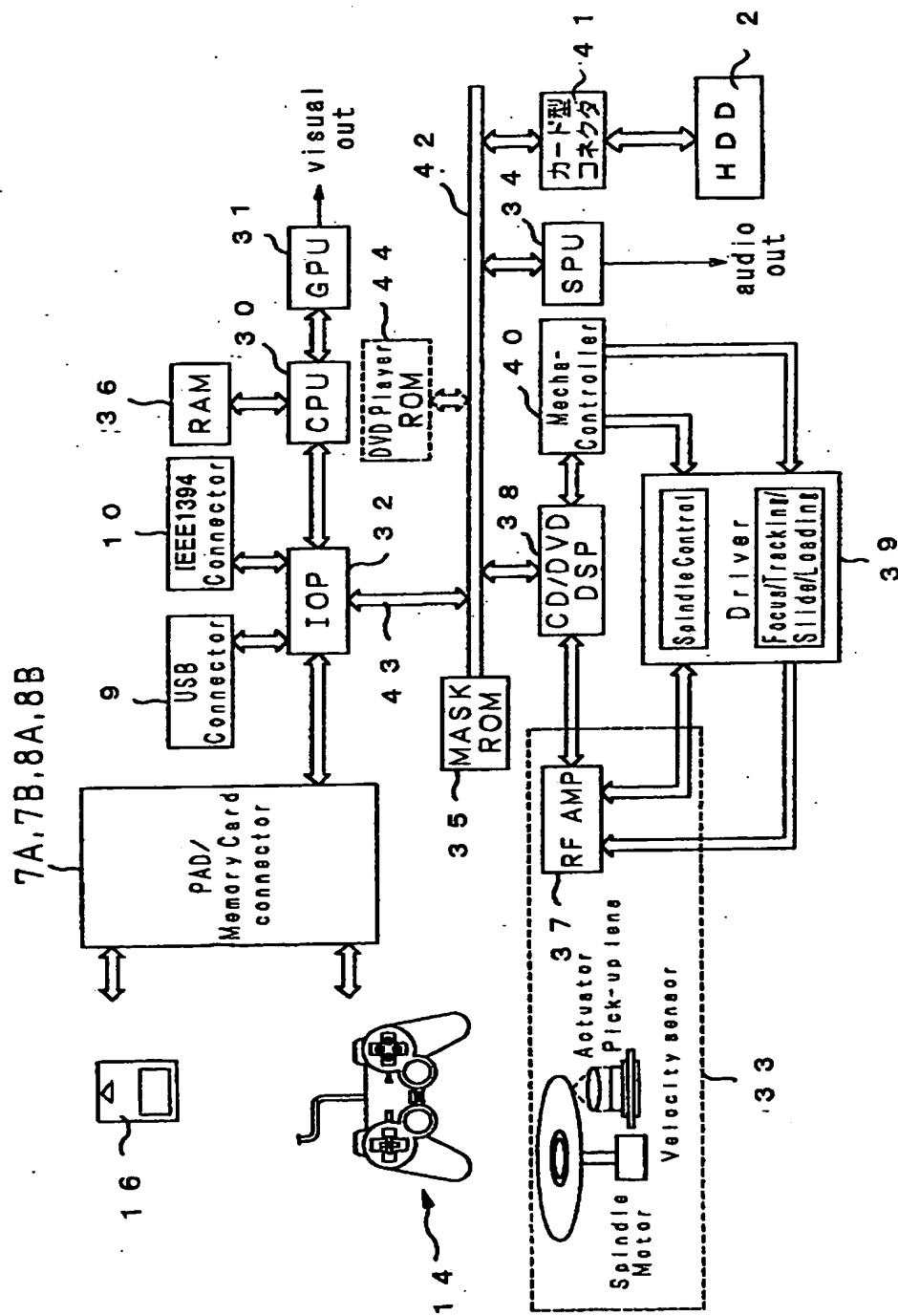
## 【図1】



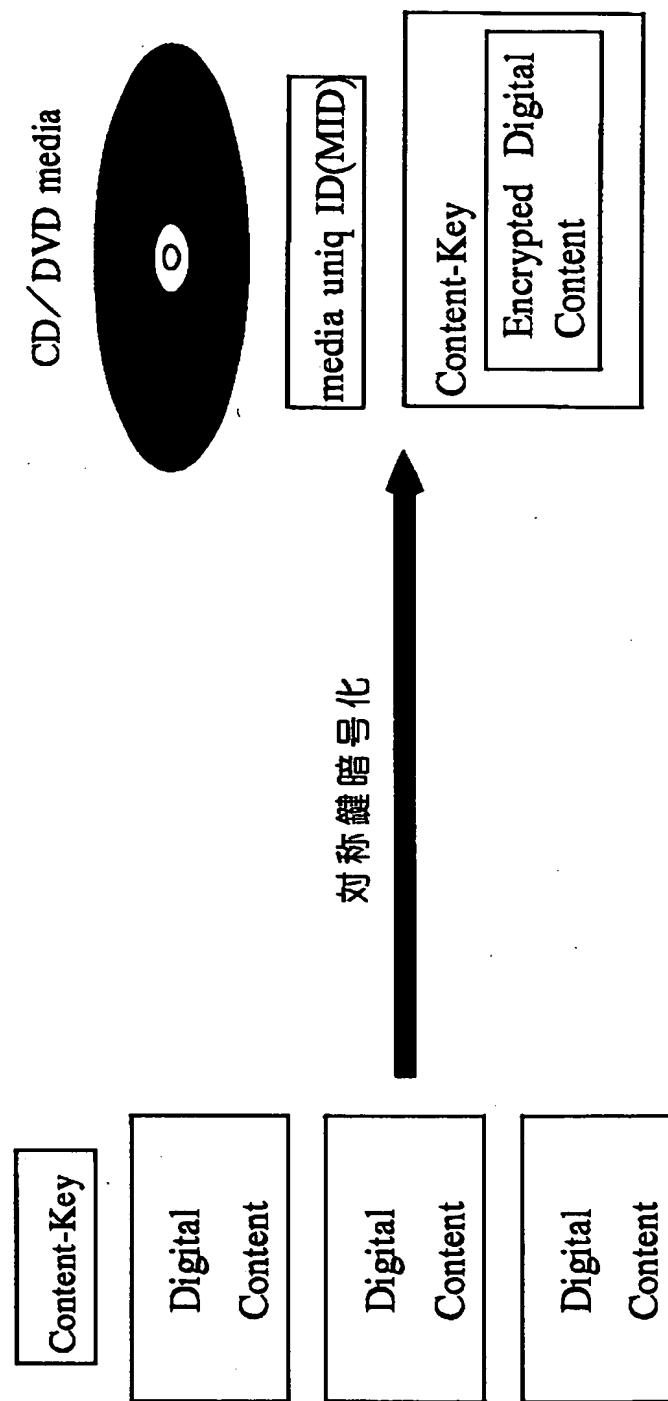
【図2】



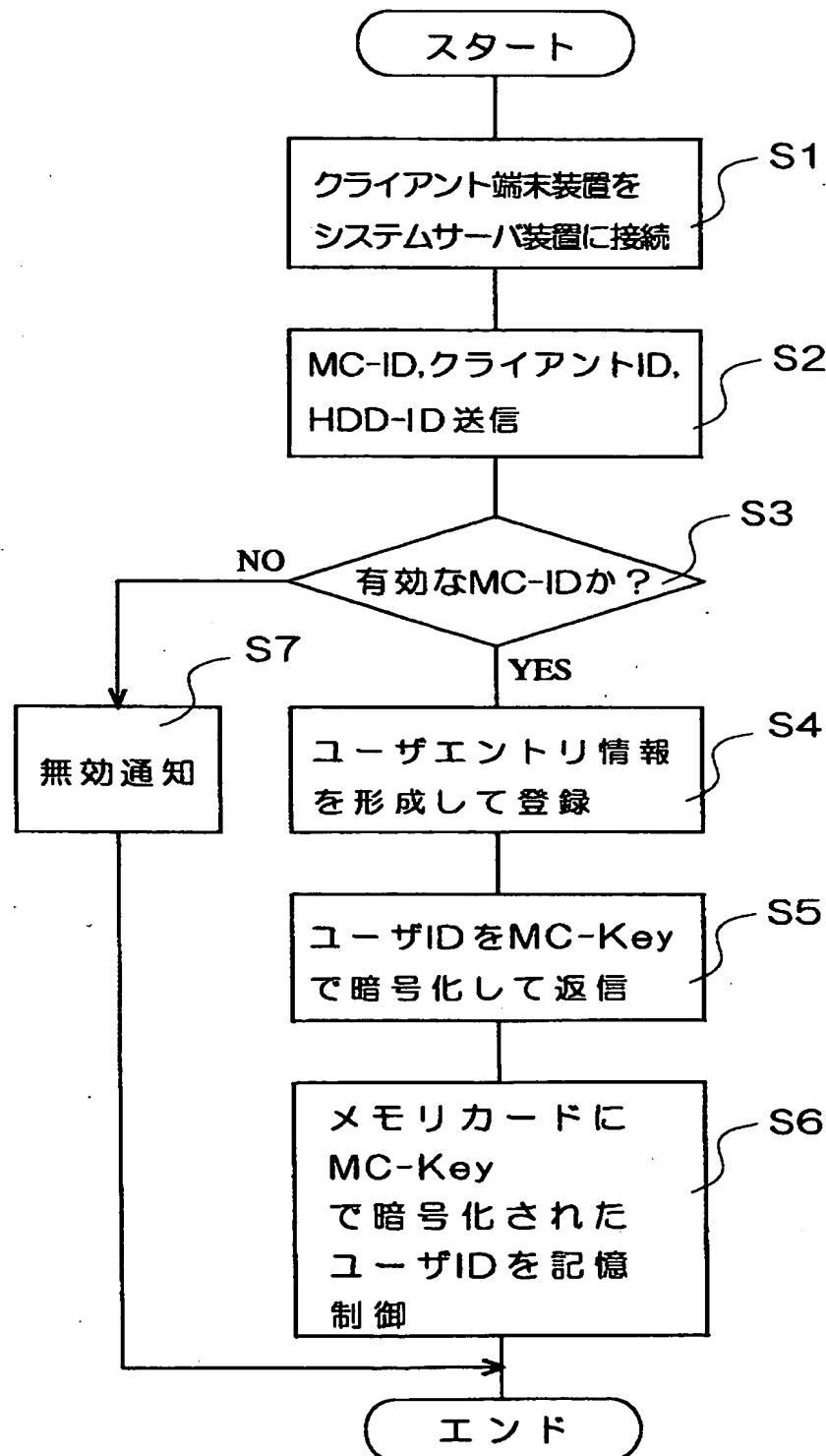
【図3】



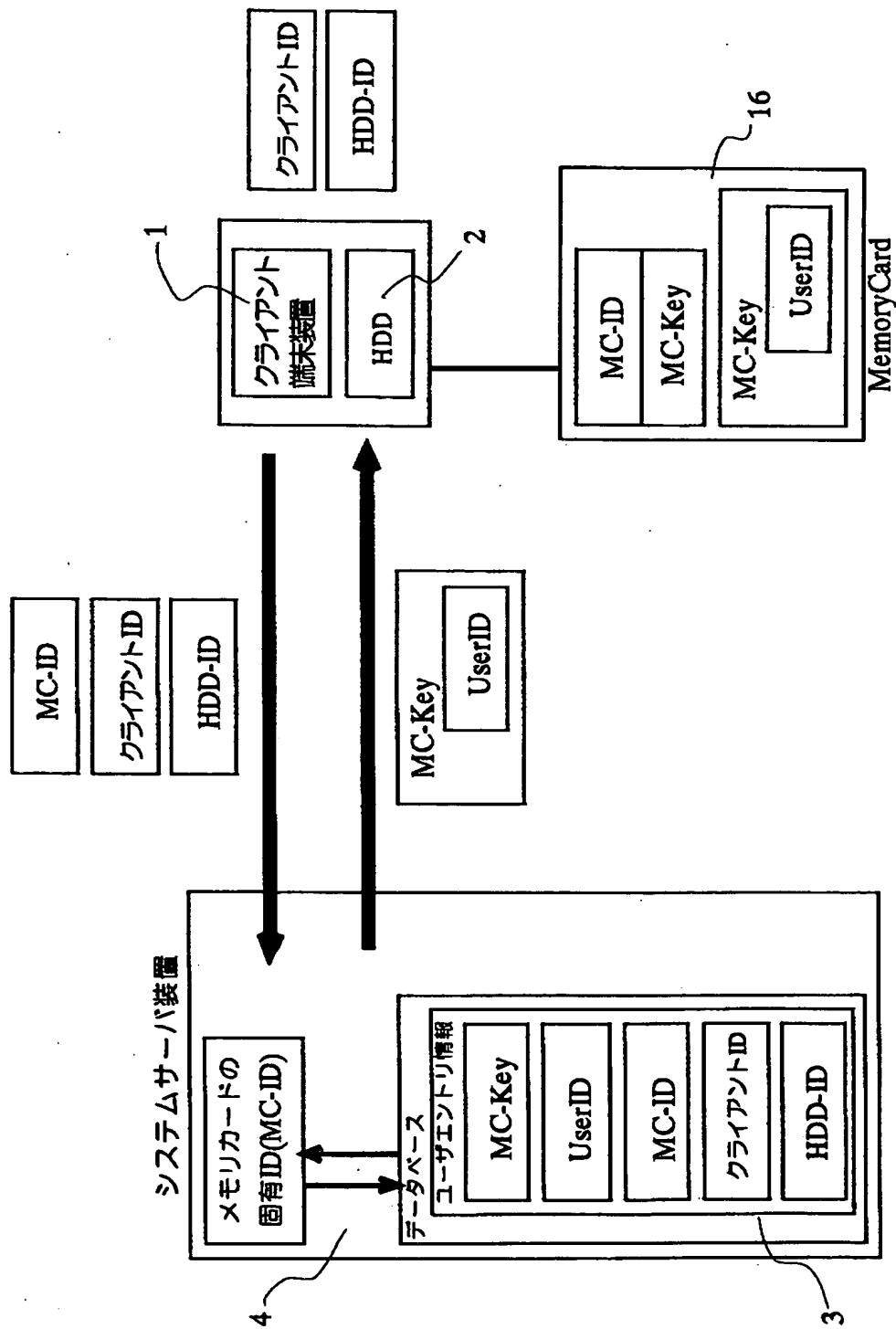
【図4】



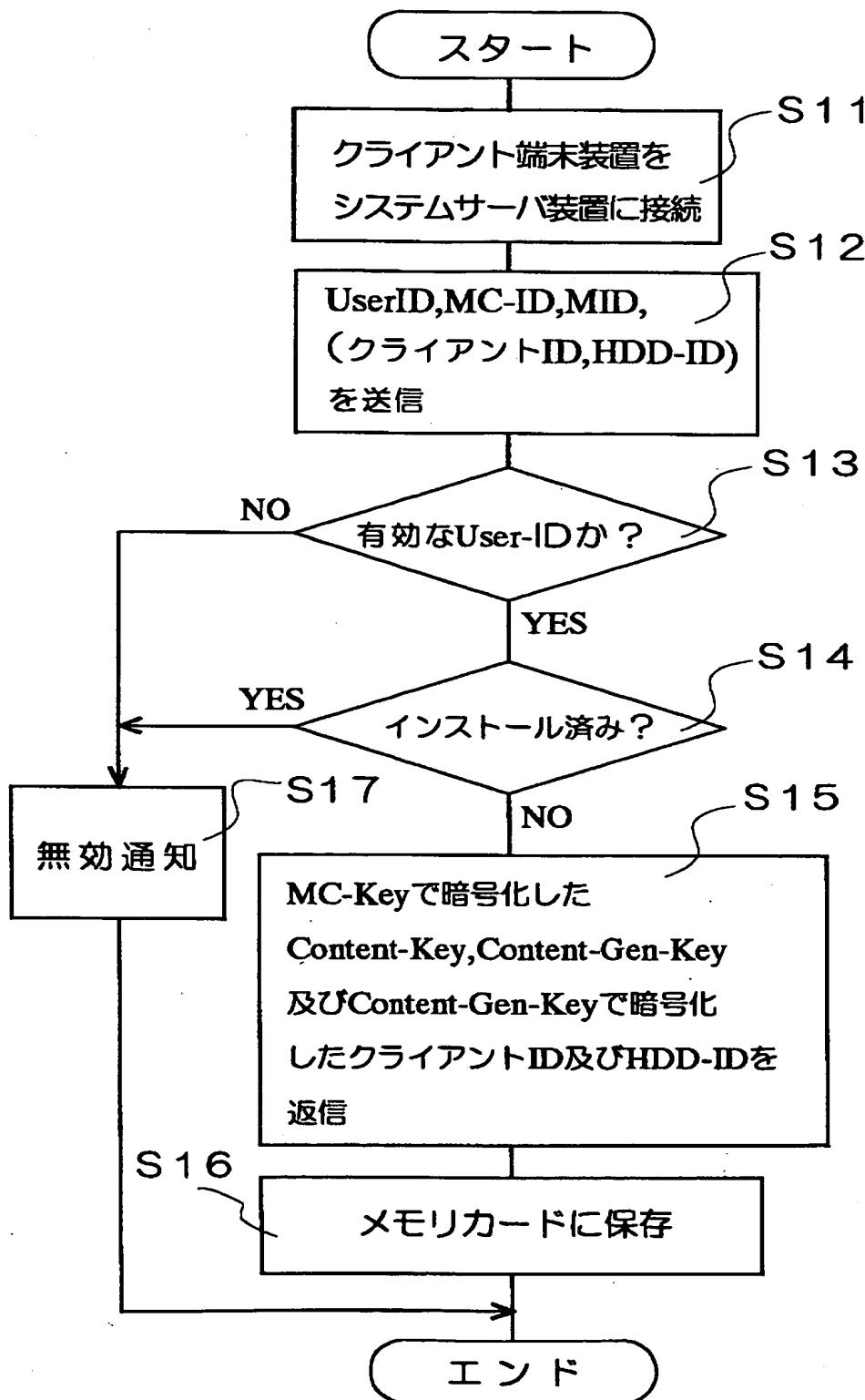
【図5】



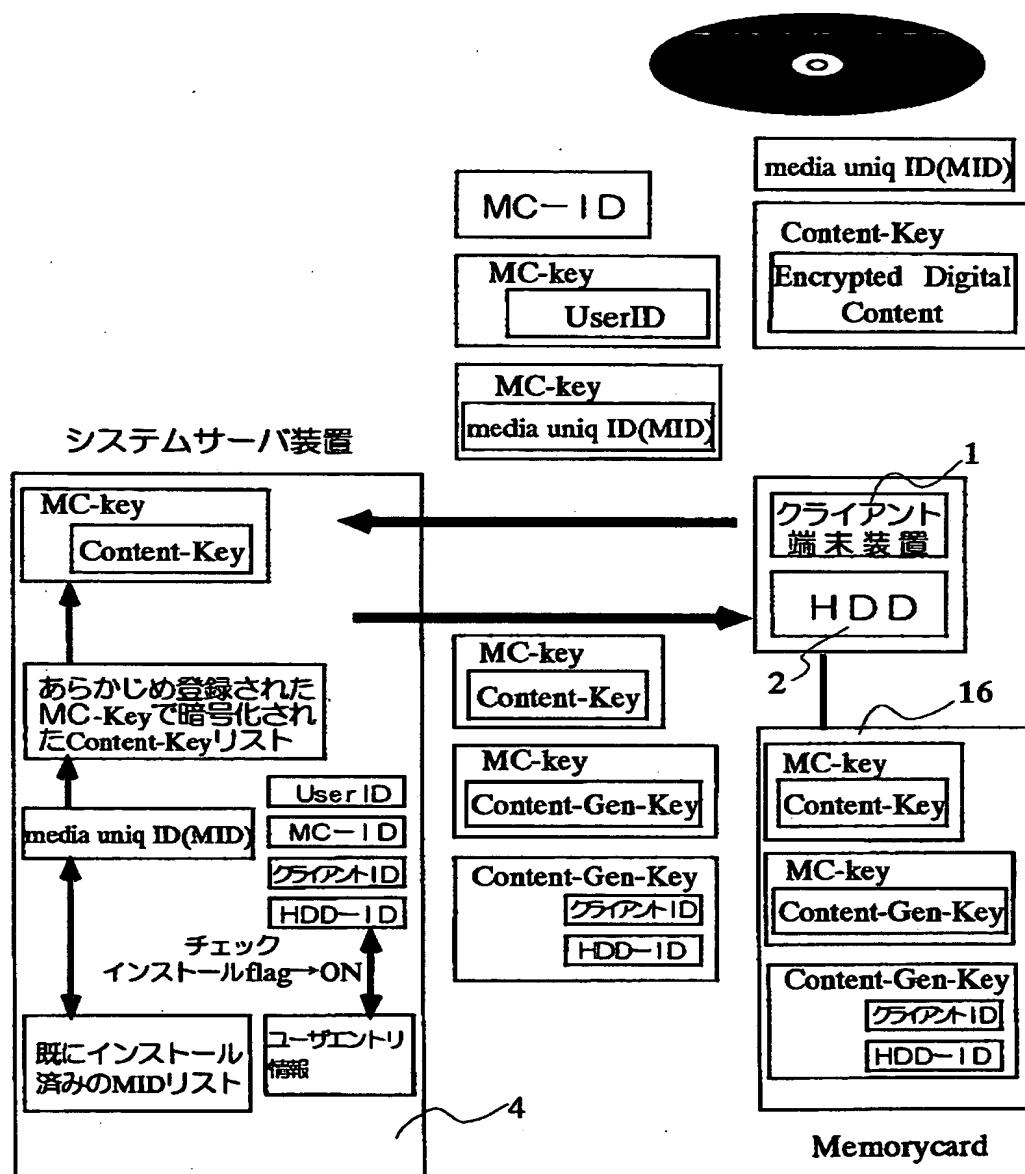
【図6】



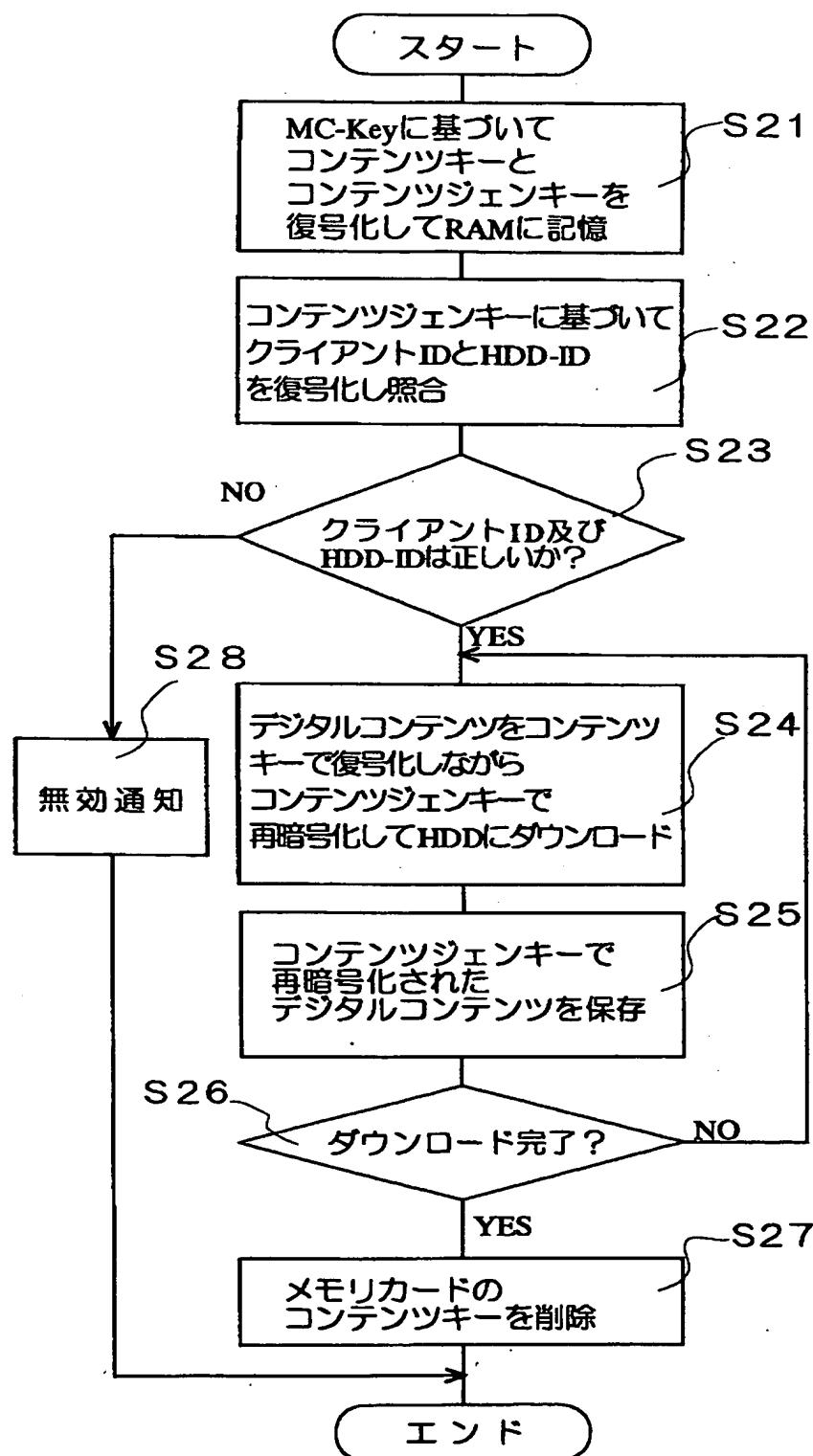
【図7】



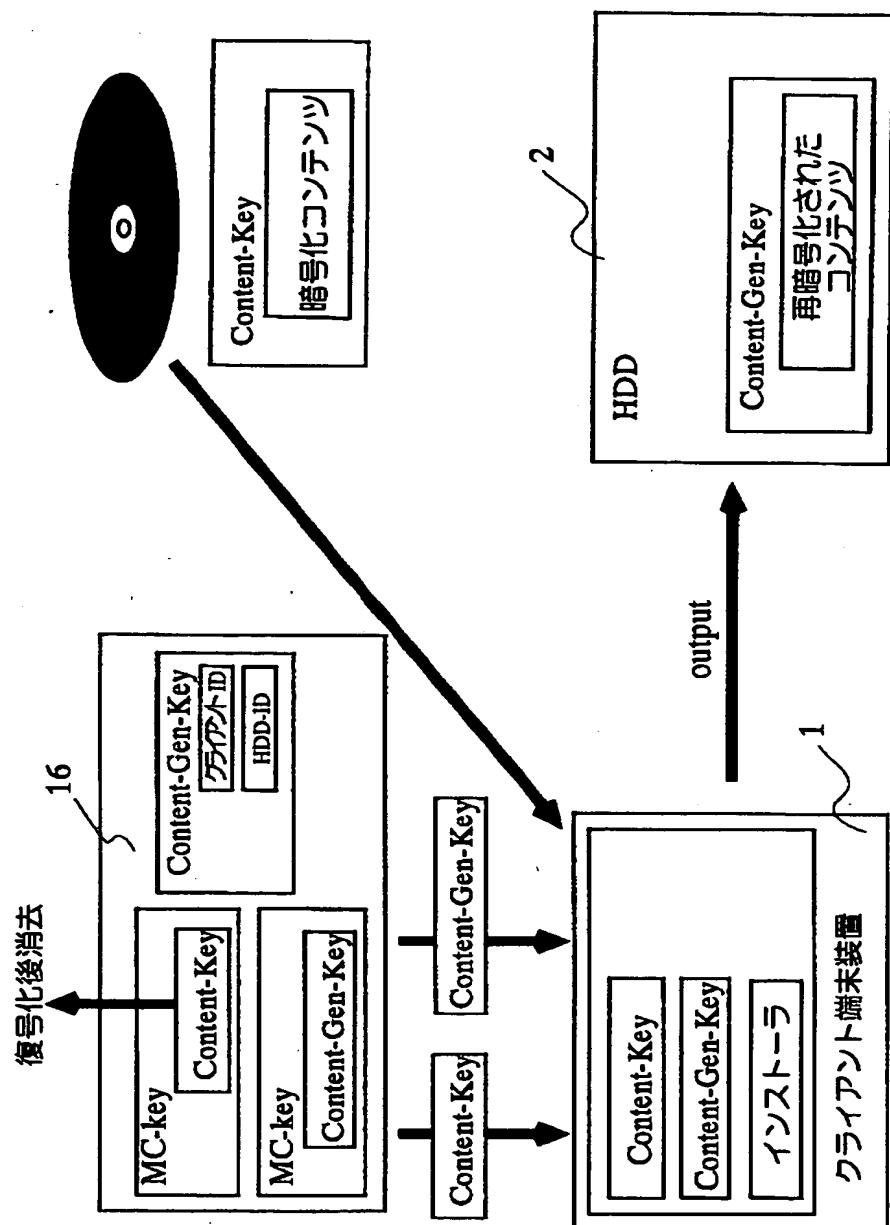
【図8】



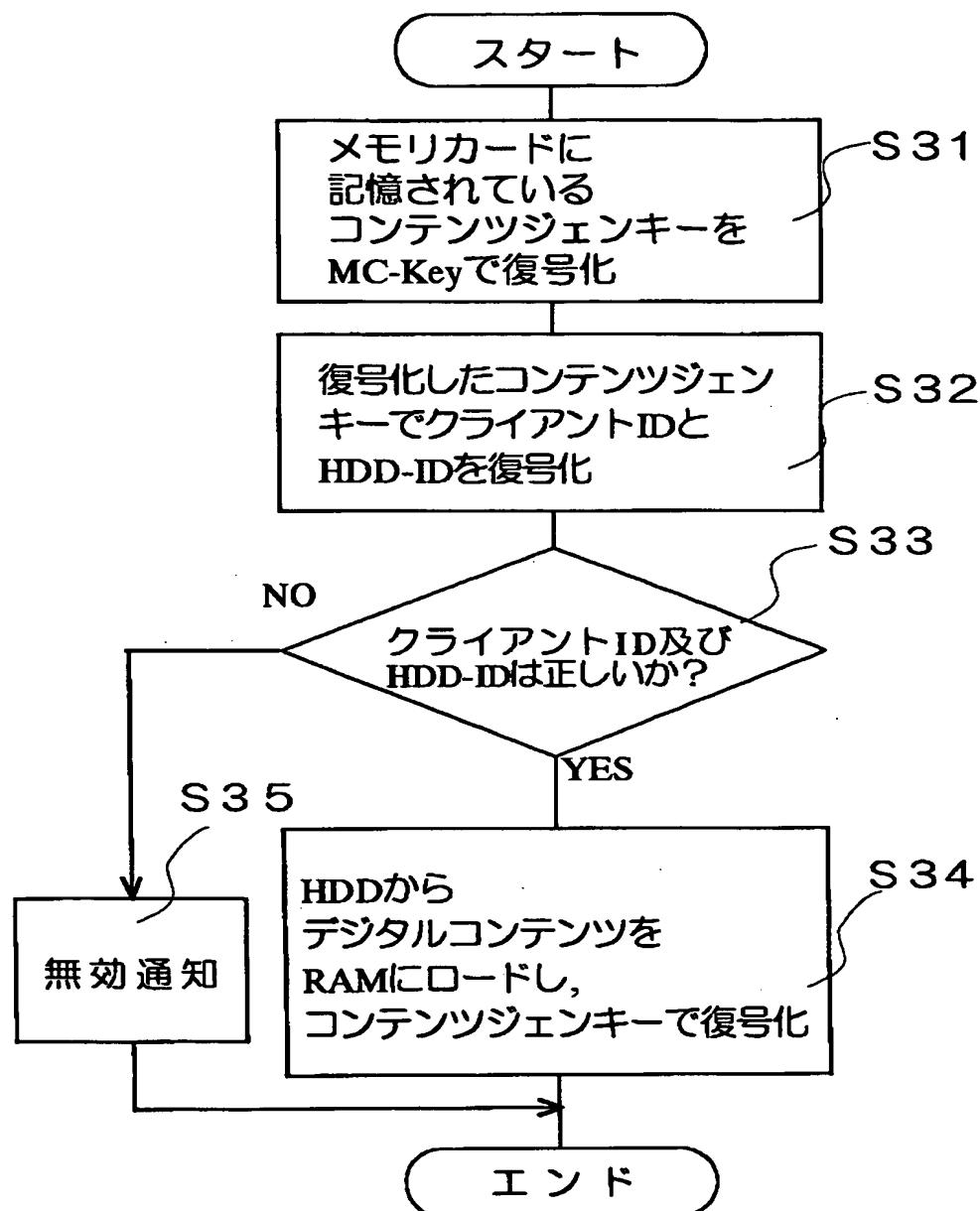
【図9】



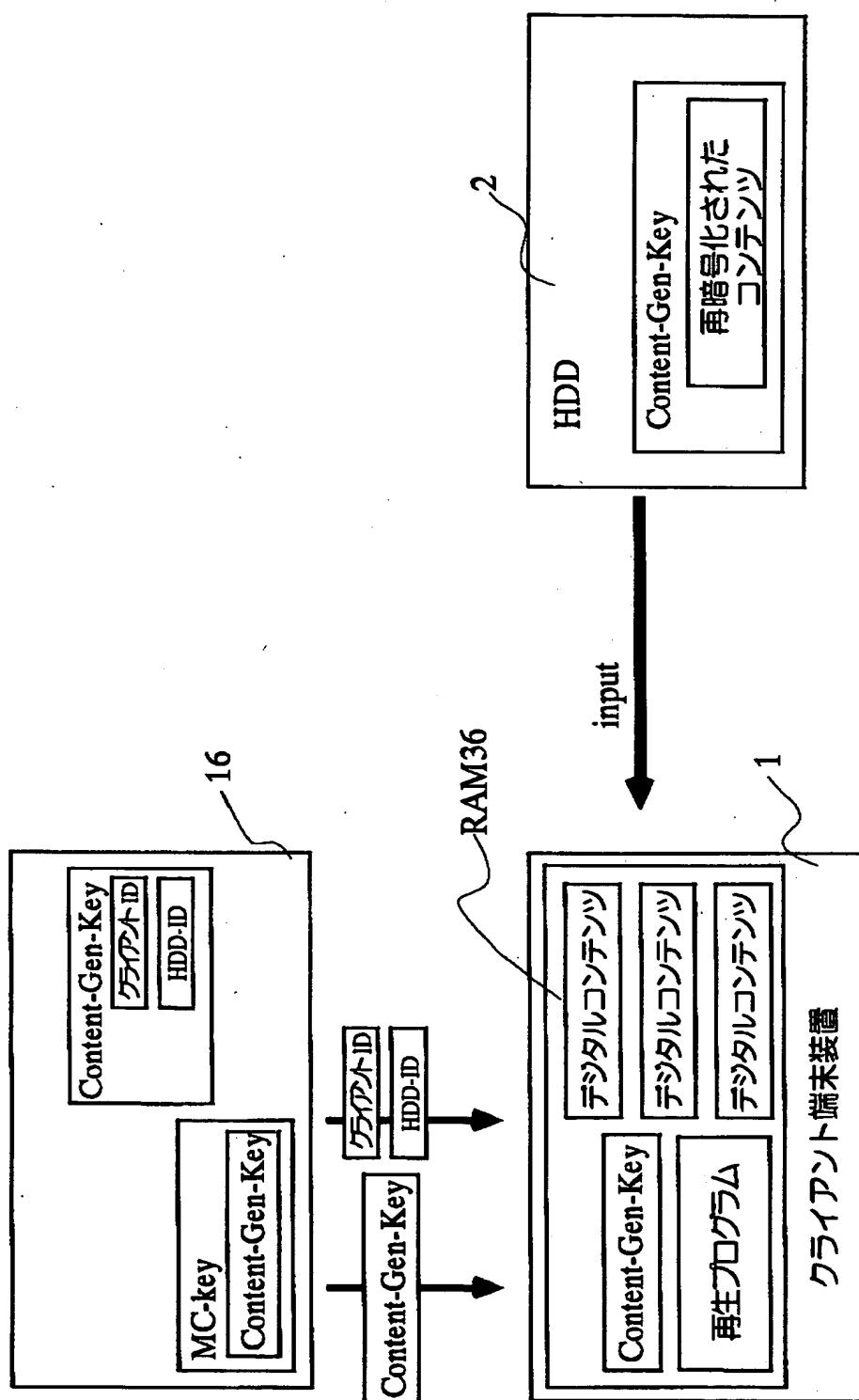
【図10】



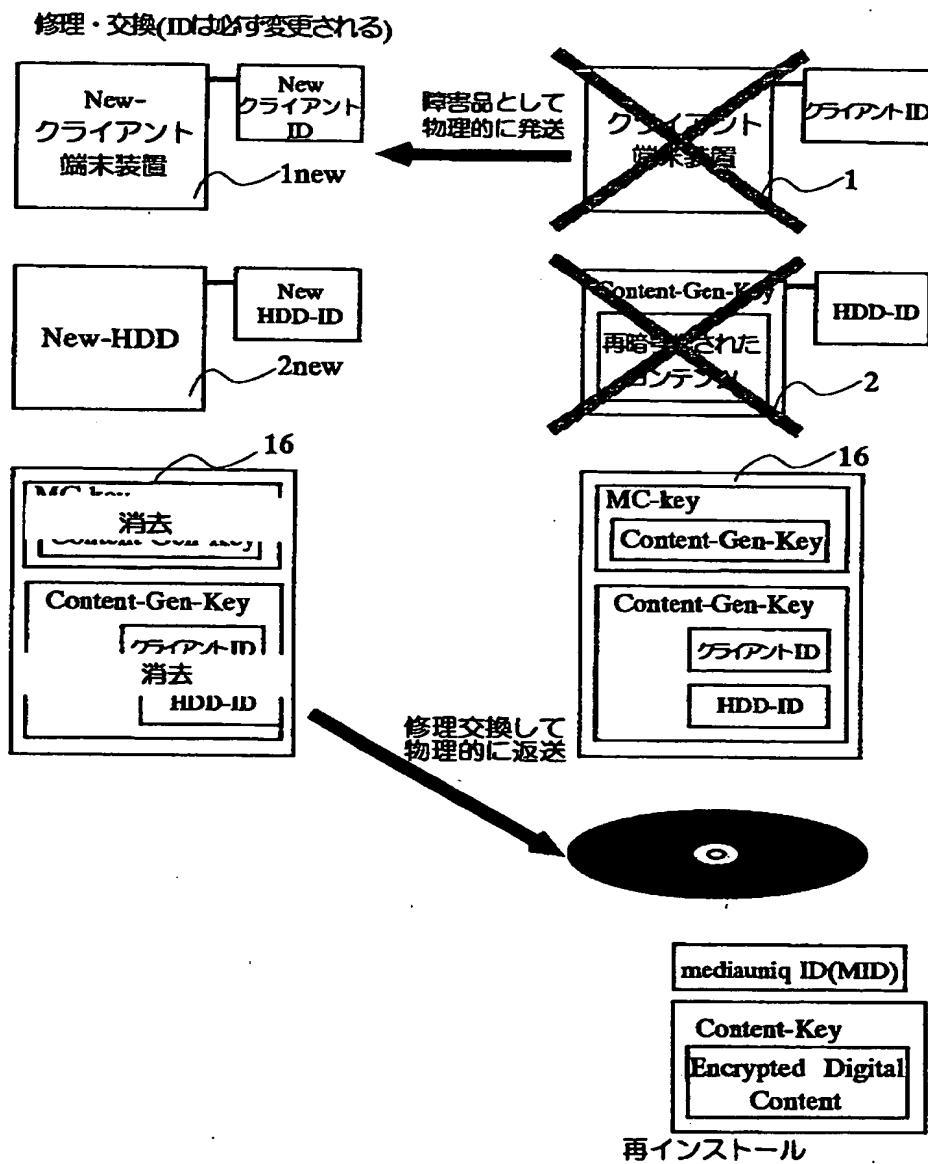
【図11】



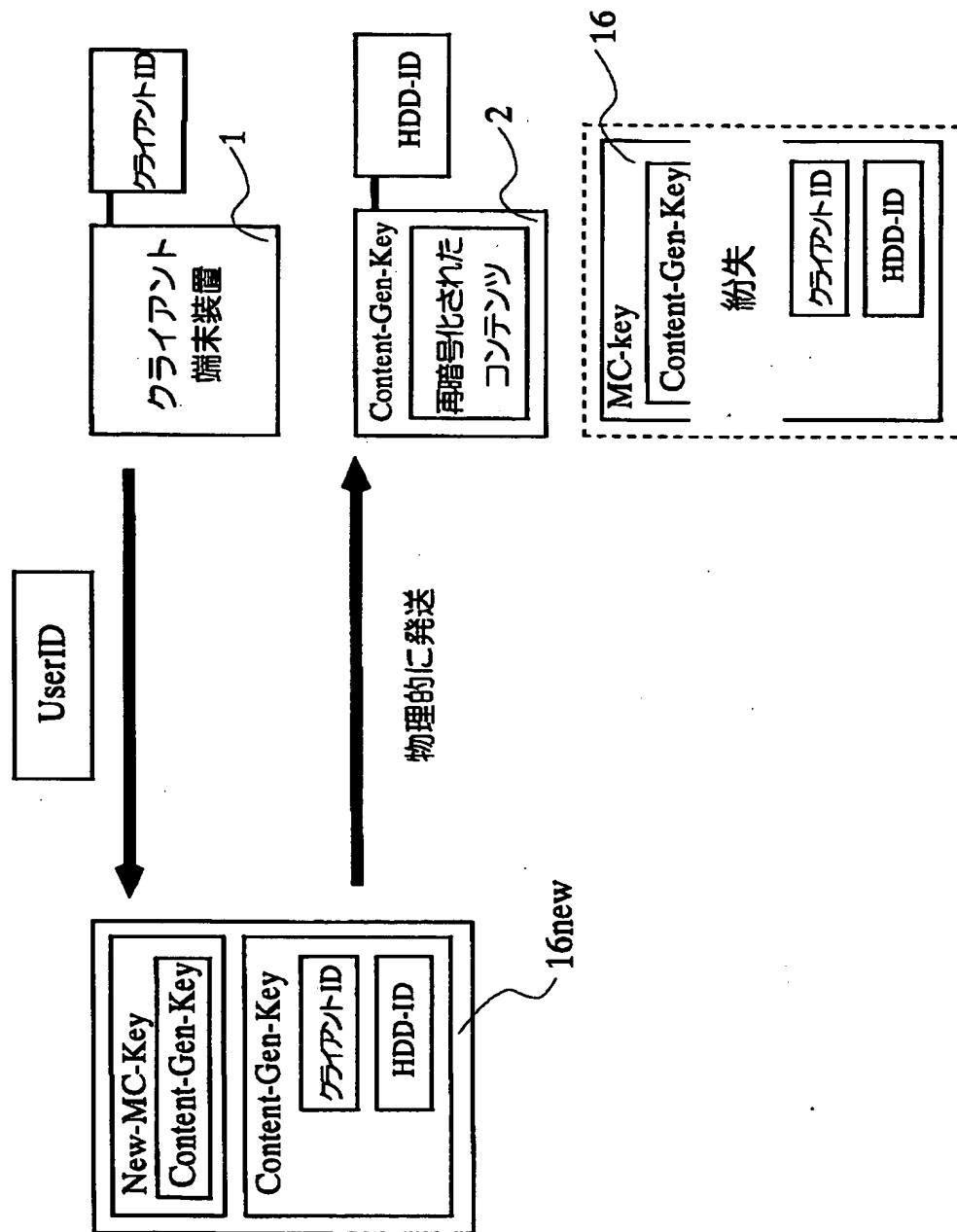
【図12】



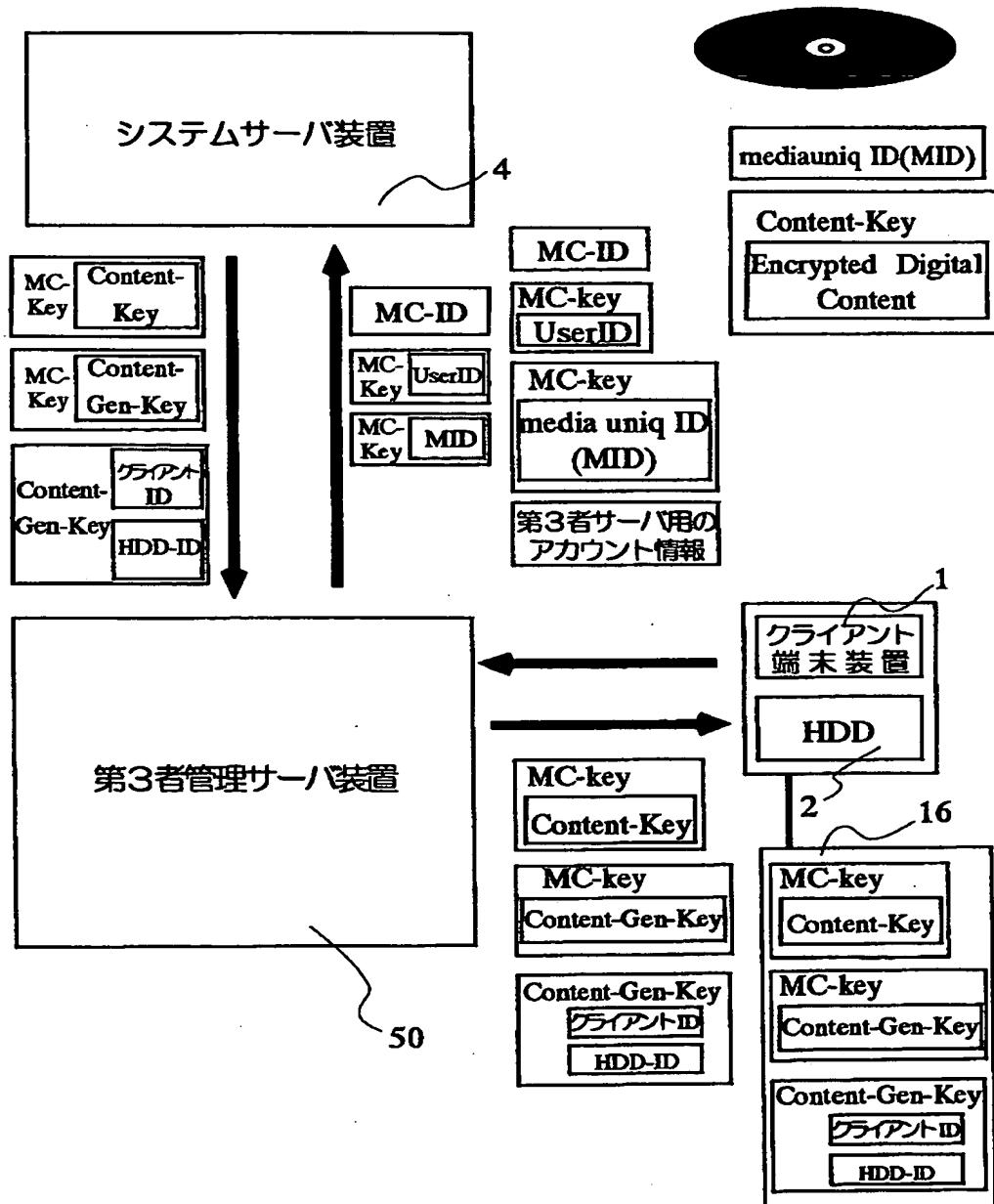
【図13】



【図14】



【図15】



【書類名】 要約書

【要約】

【課題】 正規のユーザに対してのみ光ディスクからハードディスクドライブ（HDD）へのデジタルコンテンツのダウンロードを可能として不正使用を防止する。

【解決手段】 各光ディスク毎にID（MID）を付すと共に、デジタルコンテンツをContent-Keyで暗号化して記録しておく。また、システムサーバ装置4は、ユーザが所有するクライアント端末装置1のクライアントID、HDD2のHDD-ID、及びメモリカード16のMC-ID等をユーザエントリ情報として管理する。ユーザはダウンロードを行う際に、光ディスクのMIDと共にMC-IDをシステムサーバ装置4側に送付する。システムサーバ装置4は、MC-IDをユーザエントリ情報と照合してユーザを特定し、デジタルコンテンツの暗号化の際に用いたContent-Keyを返送する。ユーザ側では、この返送されたContent-Keyを用いて光ディスクに記録されているデジタルコンテンツを復号化しHDD2にダウンロードする。

【選択図】 図8

認定・付加情報

特許出願の番号 特願2001-044358  
受付番号 50100237847  
書類名 特許願  
担当官 第七担当上席 0096  
作成日 平成13年 2月21日

<認定情報・付加情報>

【提出日】 平成13年 2月20日

次頁無

出願人履歴情報

識別番号 [395015319]

1. 変更年月日 1997年 3月31日

[変更理由] 住所変更

住 所 東京都港区赤坂7-1-1

氏 名 株式会社ソニー・コンピュータエンタテインメント